UNITED STATES DISTRICT COURT

DISTRICT OF NEW MEXICO

STATE OF NEW MEXICO *EX REL.* HECTOR BALDERAS, ATTORNEY GENERAL, Plaintiff, v. ROVIO ENTERTAINMENT CORPORATION, Defendant.	Case No. _____ **COMPLAINT** **DEMAND FOR JURY TRIAL**

TABLE OF CONTENTS

COMES NOW, the State of New Mexico, by Attorney General Hector Balderas ("the State"), who brings this Complaint against Defendant Rovio Entertainment Corporation ("Rovio" or "Defendant"), and alleges as follows:

I. INTRODUCTION

1. This action is brought to protect children in the State of New Mexico from Defendant's surreptitious acquisition of their Personal Information[1] for the purposes of tracking children over time and across the internet and targeting them for psychological and commercial exploitation.

2. Defendant Rovio develops and publishes the popular franchise of Angry Birds apps. First introduced in 2009, the apps became immensely popular with children in New Mexico and throughout the world, with simplistic gameplay in which the player launches cartoon birds from a giant slingshot in order to knock down structures built by green cartoon pigs.

[1] As used herein, "Personal Information" is any data that refers to, is related to, or is associated with an identified or identifiable individual. This includes, but is not limited to, all "Personal Information" as defined in 12 C.F.R. § 312.2 for the purposes of the Children's Online Privacy Protection Act.

Figure 1

The strength of the franchise has led to the release of more than 35 spin-off games totaling over 4.5 billion app downloads to date.

3. The most popular apps in the franchise have been downloaded anywhere from tens of millions to *billions* of times, worldwide, including upon information and belief, over one million times or more in New Mexico. These apps include: Angry Birds, Angry Birds Classic, Angry Birds 2, Angry Birds Friends, Angry Birds Transformers, Angry Birds POP!, Angry Birds Blast!, Angry Birds Evolution, Angry Birds Match, and Angry Birds Dream Blast, Angry Birds Seasons, Angry Birds Space and Angry Birds Go! (collectively, "Angry Birds Gaming Apps" or "Gaming Apps"). *See* Exhibit 1.

4. Rovio aggressively directs the Angry Birds Gaming Apps to young children in New Mexico, whom Rovio targets for financial gain in several ways, including: (1) by selling the paid Gaming Apps themselves for download; (2) by selling "virtual goods" within the Gaming Apps to prolong and enhance play; and (3) by selling "physical goods" such as children's toys and merchandise based on the popular Angry Birds Gaming Apps, that, in turn, also purposely serve as conduits (e.g. via QR codes) to downloading and playing the Angry Birds Gaming Apps themselves.

5. Beyond the apps, the Angry Birds franchise includes wide-release feature films, animated shows, fast-food tie-ins, toys, children's clothing, and more child-directed merchandise based on the characters from the apps. These franchise items were sold in New Mexico and throughout the world. Shortly after the release of the first Angry Birds app in 2009, Rovio began its strategy of selling merchandise to children in New Mexico and elsewhere, including tens of millions of stuffed Angry Birds toys by 2012.[2] By 2013, researchers identified Rovio's online games as the most addictive games for kids.[3] Over the past decade, Rovio further monetized its massive child audience by marketing scores of spinoff Angry Birds children's toys and other merchandise, including baby blankets, infant Halloween costumes, action figures, children's lunchboxes, slot cars, playground equipment, and playground balls. *See* Exhibit 2 (listing 50 nonexhaustive examples).

6. Further, Rovio released two Angry Birds feature films with a target audience of children ages 5-10, each grossing hundreds of millions of dollars worldwide, including significant box office receipts in New Mexico. In a November 2020 press release, Rovio trumpeted the immense popularity among children of its cartoon featuring the characters in (and animation style of) the Angry Birds Gaming Apps, boasting that "56% of 4-16 year olds in the US watch the Angry Birds animated series at least once or a few times a week (with 45% of kids aged 4-7 and 52% of kids aged 8-11 watching every day in the US!)."[4]

7. To be clear, there is no reasonable dispute that the Angry Birds franchise of apps is directed toward (young) children. Indeed, Rovio acknowledge this fact on its website, noting

---

[2] Jenna Wortham, *Angry Birds Migrates to Facebook and Toy Stres*, New York Times (February 13, 2012), https://bits.blogs.nytimes.com/2012/02/13/angry-birds-migrates-to-facebook-and-toy-stores/ (last accessed July 30, 2021).

[3] Perez, Sarah. "Rovio Titles Among The Most Addictive Games For Kids, Study Finds." *TechCrunch*, TechCrunch, 21 Jan. 2013, http://tcrn.ch/V1RqMk (accessed on May 12, 2021)

[4] Exhibit 7.

"[k]ids love playing our games. We strive to create fun and engaging games that people of all ages can enjoy, and we're totally jazzed that so many young kids gravitate towards our titles."[5]

8. Rovio monetizes children by surreptitiously exfiltrating their personal information while they play the Angry Birds Gaming Apps and then using that personal information for commercial exploitation. When children play the Angry Birds Gaming Apps on their mobile devices, their online activity and other Personal Information are inescapably—and without verifiable parental consent—exfiltrated to third parties and their marketing networks in order to target the children with advertisements based on their own personal information. This conduct endangers the children of New Mexico, undermines the ability of their parents to protect children and their privacy, and violates state and federal law.

9. While most children and their parents think that the Angry Birds Gaming Apps are innocent, online games—the digital equivalent of puzzles, blocks, or books—Rovio has embedded coding in the apps that allows them to exfiltrate children's data as they play. These pieces of code are called software development kits (or "SDKs") and are designed and implemented by internet advertising companies. Once embedded, these advertising companies use the SDKs to affirmatively exfiltrate the child user's Personal Information, sending data and advertisements back and forth. The SDK sends the child's data back to the advertising companies, where it is analyzed, stored, and used to build increasingly detailed profiles of child users. In turn, Rovio and its ad-tech partners, provide and transfer the data to myriad third parties around the world so that each can continue to build their own profiles of child users. This activity serves one primary purpose: to learn more about the children playing the Angry Birds Gaming Apps to monetize them and send them targeted advertisements.

---

[5] Rovio, *How Can I Stop My Child From Making In-App Purchases Without Permission?*, (2018) available at https://info.rovio.com/hc/en-us/articles/360000982888-For-Apple-iOS- (for Apple iOS devices); https://info.rovio.com/hc/en-us/articles/360000982868-For-Google-Play-Android (for Google Play Android devices); https://info.rovio.com/hc/en-us/articles/360000972707-For-Amazon-Android- (for Amazon Android devices) (last accessed July 30, 2021).

10. Defendant, in conjunction with the hidden SDKs embedded in its apps, exfiltrates the Personal Information of children who play the Angry Birds Gaming Apps in New Mexico—the very audience for whom the apps are designed—and uses that data for commercial gain, without obtaining verifiable parental consent for their activities. This conduct is not passive in nature, but purposely and specifically targets children in the State of New Mexico in violation of federal and state law.

11. The risks associated with exfiltration of Personal Information apply with greatest force when children's privacy is at stake. Children have a long- and widely-recognized vulnerability to commercial exploitation which can be—and here is—exploited through the immediacy and ease with which information can be collected from them, and the ability of the online medium—including apps on smartphones and tablets—to circumvent the traditional gatekeeping role of their parents and guardians. Children also have a more difficult time differentiating between advertisements and content, a risk exacerbated by the highly-targeted nature of behavioral advertising.

12. Federal law prohibits this conduct. Recognizing the potential harms that sophisticated advertising could inflict upon children, Congress enacted the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501, et seq. ("COPPA"). COPPA empowers parents—through enforcement actions brought by a State Attorney General or the FTC—to protect their children in the online marketplace. COPPA prohibits websites or online services from collecting personal information from children under the age of 13 without first obtaining verifiable parental consent. Specifically, COPPA requires websites and online services: (1) to provide complete disclosure of the information they collect from children and how they use that information; (2) to ensure that disclosure is provided directly to parents; and (3) to obtain verifiable consent from the parent before collecting, using, or disclosing any personal information from children. Without first

complying with these requirements, the online tracking of children is illegal. Rovio has violated each one of these requirements mandated by COPPA.

13. In addition to violating COPPA, the above acts and practices violate New Mexico's Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-1, *et seq.* Defendant relentlessly, repeatedly, and willfully targeted children and surreptitiously harvested their personal information for psychological and commercial exploitation for over a decade. This justifies assessing civil penalties of up to $5,000 for each and every violation of the UPA.

14. Defendant's tracking and profiling of New Mexico children also violates the common-law tort of intrusion upon seclusion. The surreptitious and intentional monitoring, tracking, and profiling of children—in direct violation not only of federal law but of longstanding societal norms—is egregious and highly offensive conduct.

II. PARTIES

15. This action is brought for and on behalf of the sovereign State of New Mexico, by and through its duly elected Attorney General, Hector Balderas. The Attorney General, as chief legal officer of the State, is statutorily authorized to initiate and prosecute any and all suits deemed necessary for the protection of the interests and rights of the State. *See* N.M. Stat. Ann. § 8-5-2(B). Specifically, the Attorney General is authorized to initiate and prosecute suits to penalize conduct that constitutes an unfair or deceptive trade practice. *See* N.M. Stat. Ann. §§ 57-12-1 *et seq.* The Attorney General is also charged with the duty of guardian of the public interest, which includes protecting the privacy interests of New Mexico's citizens and the welfare of New Mexico's children online. The State brings this action in its *parens patriae* and/or sovereign capacity.

16. Defendant Rovio Entertainment Corporation ("Rovio") is a global mobile game development company headquartered Helsinki, Finland, with additional offices and employees during the relevant time period in the United States, in addition to at least Sweden, Denmark,

Canada, the United Kingdom, and China.[6] Rovio targeted its Angry Birds Gaming Apps (and its data-exfiltrating software) at children it knew were located in New Mexico, knowingly exfiltrated the children's data from devices located in New Mexico, injuring them in New Mexico. As detailed below, Rovio purposefully conducts business in New Mexico by affirmatively marketing Angry Birds Gaming Apps to children in New Mexico, purposefully and knowingly deploying data-exfiltrating software on children's mobile devices in New Mexico and affirmatively exfiltrating children's Personal Information from those devices in New Mexico. Since at least 2009, with the release of its first Angry Birds app, Rovio has engaged in the business of developing and publishing numerous Angry Birds Gaming Apps for children to download to devices located in New Mexico and has marketed these apps in New Mexico, including by working with U.S. advertisers, contracting with U.S. ad networks (as defined *infra*), embedding advertisers' software into its apps, and integrating U.S. social media platforms into its apps. Rovio knowingly and purposefully has released its Angry Birds Gaming Apps, as well as its attendant merchandise based on those apps (including the numerous toys, children's clothing, lunchboxes, etc. detailed below),[7] its animated shows, and its feature length movies into the stream of commerce in the State of New Mexico, both through online and brick-and-mortar retailers (*e.g.* Burger King, Wal-Mart, Target, Best Buy etc.) located in New Mexico. In so doing, Defendant Rovio further partners with US-based toy companies (including but not limited to Hasbro and Mattel), media companies (including but not limited to Sony Pictures, Columbia Pictures, and YouTube), advertising companies (including but not limited to the advertising SDKs identified herein), fast food companies (including but not limited to Burger King), and retailers (including but not limited to Walmart, Target, and Amazon), in order to sell its products and services throughout the United States, generally, and in New Mexico, specifically.

[6] https://investors.rovio.com/en/about-us/who-we-are (last accessed July 30, 2021).
[7] *See* Exhibit 2.

III. JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1367.

18. This Court has personal jurisdiction pursuant to 15 U.S.C. § 6504(e)(2) which authorizes nationwide service of process in actions under COPPA. *See also* 15 U.S.C. § 6504(a)(1)("In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates any regulation of the [Federal Trade] Commission prescribed under [COPPA], the State, as *parens patriae*, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction.").

19. Rovio markets and sells its Angry Birds Gaming Apps and related merchandise in New Mexico, both online and in brick-and-mortar stores. Further, Rovio utilizes and has utilized code in the Gaming Apps on children's devices in New Mexico and, via those devices and that code, affirmatively collects and sends (and has collected and sent) those children's Personal Information to its own servers (as well as its agents' and partners' servers) as children play on their devices in New Mexico, in order to request advertisements targeted to those children.

20. This Court also has personal jurisdiction over Defendant pursuant to N.M. Stat. Ann. § 38-1-16 because Defendant engages in consumer transactions within the State of New Mexico; purposefully directs and/or directed its actions toward the State of New Mexico; tracks children by siphoning persistent identifiers and other Personal Information as they play Rovio's Angry Birds Gaming Apps in, and move about, New Mexico; and/or has the requisite minimum contacts within the State of New Mexico needed to permit this Court to exercise jurisdiction.

21. In accordance with 28 U.S.C. § 1391, venue is proper in this district because a substantial part of the conduct giving rise to the State's claims occurred in this District, and because Defendant transacts business in this District.

IV. ALLEGATIONS APPLICABLE TO ALL COUNTS[8]

A. COPPA Outlaws the Collection of Personal Information of Children Under Age 13 from Child-directed Apps Without Verifiable Parental Consent.

22. Children are especially vulnerable to online tracking and the resulting behavioral advertising and user profiling. While children's cognitive abilities are still developing, they have limited understanding and awareness of sophisticated advertising and are therefore less likely than adults to distinguish between the actual content of online Angry Birds Gaming Apps and the advertising content that is targeted to them alongside it. Thus, children may engage with advertising content without realizing they are doing so.[9]

23. Recognizing this vulnerability, Congress enacted COPPA, with the express goal to "place parents in control over what information is collected from their young children online."[10]

24. COPPA "prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet." 16 C.F.R. § 312.1. Specifically, it is "unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the [relevant] regulations" prescribed by the FTC. 15 U.S.C. § 6502(a)(1). COPPA provides that the

---

[8] For the Court's convenience, the State has attached a glossary of relevant terms and statutory definitions pertaining to COPPA and to the online advertising ecosystem. Said glossary is appended as Exhibit 6.

[9] *See* Comments of The Center for Digital Democracy, et al., FTC*, In the Matter of Children's Online Privacy Protection Rule* at 13-14 (Dec. 23, 2011).

[10] *See* General Questions about the COPPA, FAQ 1, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0#A.%20General%20Questions (last accessed on May 31, 2021).

operator must "obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children." 16 C.F.R. §§ 312.3(b), 312.4(a).

25. Thus, under COPPA, developers of child-directed apps, and any third parties working on the developers' behalf, are prohibited from traditional data harvesting practices endemic to the online advertising ecosystem unless they first *alert* parents to fact that data will be collected, and then obtain the *verifiable* consent of the parent to do so. 16 C.F.R. §§ 312.4, 312.5.

26. As discussed in further detail below, such verifiable consent must be informed and meaningful—COPPA requires more than checking a box in a "clickwrap" agreement[11] or posting an inconspicuous hyperlink to a privacy policy that a user may or may not peruse. Instead, there must be a strong, objective record of a parent's consent to her child being tracked.

27. Under COPPA, operators (e.g., app developers like Rovio) whose content is directed to children are strictly liable if personal information is collected, used, and/or disclosed from children under 13. 16C.F.R. § 312.2. Operators are also strictly liable if personal information is collected or maintained on their behalf, which COPPA defines as when "[t]he operator benefits by allowing another person to collect personal information directly from users of" an online service. *Id.*

28. Ad networks and other SDK entities also may be held liable for collecting personal information from child users under COPPA, if they have "actual knowledge" that the apps using their software development kits are directed to children. *Id.*

29. COPPA defines "personal information" broadly as follows:

> individually identifiable information about an individual collected online,

[11] Clickwrap agreements require a user to affirmatively click a box on a website acknowledging agreement to the terms of service before the user is allowed to proceed. *See* "From the Chair: 'Click Here to Accept the Terms of Service,'" American Bar Association Communications Lawyer Newsletter, Vol. 31 No. 1 (January 2015), https://www.americanbar.org/publications/communications_lawyer/2015/january/click_here.html) (last accessed July 30, 2021).

> including (1) a first and last name; (2) a home or other physical address including street name and name of a city or town; (3) online contact information [separately defined as "an email address or any other substantially similar identifier that permits direct contact with a person online"]; (4) a screen name or user name…; (5) telephone number; (6) a Social security number; (7) ***a persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier"***); (8) a photograph, video, or audio file where such file contains a child's image or voice; (9) Geolocation information sufficient to identify street name and name of a city or town; or (10) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

16 C.F.R. § 312.2 (emphases added). Persistent identifiers are the "personal information" of greatest value and utility for tracking, profiling, targeting, and monetizing children and others generally on the Internet.

30. The FTC regards "persistent identifiers" as "personally identifiable" information that can be reasonably linked to a particular child. The FTC amended COPPA's definition of "personal information" to clarify the inclusion of persistent identifiers.

B. COPPA Requires Providing Direct, Online Notice, and Verifiable Parental Consent.

31. In order to collect, use, or disclose personal information lawfully (including persistent identifiers), COPPA requires that an operator like Rovio meet specific requirements, including *each* of the following:

Direct Notice to the Parent

32. It is not enough that an operator simply has a free-standing privacy policy or terms of service on a website or in an app. COPPA requires that an operator use "reasonable efforts" to provide *direct* notice to parents prior to obtaining a child's personal information. Specifically, "[a]n operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any

material change in the collection, use, or disclosure practices to which the parent has previously consented." 16 C.F.R. § 312.4(b). This notice must contain the following information:

a. That the operator has collected the parent's online contact information from the child, and, if such is the case, the name of the child or the parent, in order to obtain the parent's consent;

b. That the parent's consent is required for the collection, use, or disclosure of such information, and that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide such consent;

c. The additional items of personal information the operator intends to collect from the child, or the potential opportunities for the disclosure of personal information, should the parent provide consent;

d. A hyperlink to the operator's online notice of its information practices;

e. The means by which the parent can provide verifiable consent to the collection, use, and disclosure of the information; and

f. That if the parent does not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the parent's online contact information from its records.

16 C.F.R. § 312.4(c)(1).

Online Notice

33. "In addition to the direct notice to the parent, an operator must post a prominent and clearly labeled link to an online notice of its information practices with regard to children . . . . [t]o be complete, the online notice of the Web site or online service's information practices must state the following:

a. The name, address, telephone number, and email address of all operators collecting or maintaining personal information from children through the Web site or online service. Provided that: The operators of a Web site or online service may list the name, address, phone number, and email address of one operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or maintaining personal information from children through the Web site or online service are also listed in the notice;

b. A description of what information the operator collects from children, including whether the Web site or online service enables a child to make personal information publicly available; how the operator uses such information; and, the operator's disclosure practices for such information; and

c. That the parent can review or have deleted the child's personal information, and refuse to permit further collection or use of the child's information, and state the procedures for doing so."

16 C.F.R. § 312.4(d) (emphasis added).

Verified Parental Consent

34. Broadly, "[a]n operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented." 16 C.F.R. § 312.5(a)(1).

35. But this consent may not be presented as an all-or-nothing proposition. Instead, "[a]n operator must give the parent the option to consent to the collection and use of the child's

personal information without consenting to disclosure of his or her personal information to third parties." 16 C.F.R. § 312.5(a)(2).

36. "An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent." 16 C.F.R. § 312.5(b)(1).

37. The FTC has identified the following methods as acceptable ways to obtain verifiable parental consent: (i) providing a consent form for parents to sign and return; (ii) requiring the use of a credit card/online payment that provides notification of each transaction; (iii) connecting to trained personnel via video conference; (iv) calling a staffed toll-free number; (v) providing a copy of a form of government issued ID that you check against a database (to be deleted upon verification); (vi) asking knowledge-based questions; or (vii) verifying a photo ID from the parent compared to a second photo using facial recognition technology. 16 C.F.R. § 312.5(b)(2).[12]

C. Rovio's Angry Birds Gaming Apps are Child-Directed.

38. The Angry Birds Gaming Apps are available for download in online app stores, including the Google Play Store ("Google Play"). In 2009 Rovio released its first Angry Birds Gaming App—the original "Angry Birds" game—which subsequently became a franchise that includes over 35 gaming apps that have been downloaded over 4.5 billion times worldwide. These apps include: Angry Birds, Angry Birds Classic, Angry Birds 2, Angry Birds Friends, Angry Birds Transformers, Angry Birds POP!, Angry Birds Blast!, Angry Birds Evolution, Angry Birds Match,

[12] *See also* "Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business," Federal Trade Commission, https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance (last accessed July 30, 2021).

Angry Birds Dream Blast, Angry Birds Seasons, Angry Birds Space, and Angry Birds Go! *See* Exhibit 1.

39. Rovio aggressively markets its Angry Birds Gaming Apps to children, and presents each of these apps with an "Everyone" rating in the Google Play Store. *Id.* Google Play ratings "are intended to help consumers, especially parents, identify potentially objectionable content that exists within an app" and are based on the app developer's responses to questionnaires provided by Google—*i.e.* the ratings reflect the developer's representations about the appropriate audience for the app.[13] An "Everyone" rating means the app's content is "generally suitable for all ages" and "[m]ay contain minimal cartoon, fantasy or mild violence and/or infrequent use of mild language."[14]

40. COPPA identifies specific criteria for determining whether an app is "directed to children," including: "its subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the Web site or online service, as well as whether advertising promoting or appearing on the Web site or online service is directed to children." 16 C.F.R. § 312.2. Additionally, "competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience" may be considered. *Id*.

41. Google created guidance for developers that adopts a comparable rubric. In a blog post titled "Creating Apps and Games for Children and Families,"[15] it uses the following illustration of sample apps that might appeal to children, children & adults, or simply adults:

---

[13] "Play Console Help," Google https://support.google.com/googleplay/android-developer/answer/188189?hl=en (last accessed July 30, 2021).

[14] *Id.*

[15] Google, *Creating apps and games for children and families*, https://developer.android.com/google-play/guides/families (last accessed July 30, 2021).

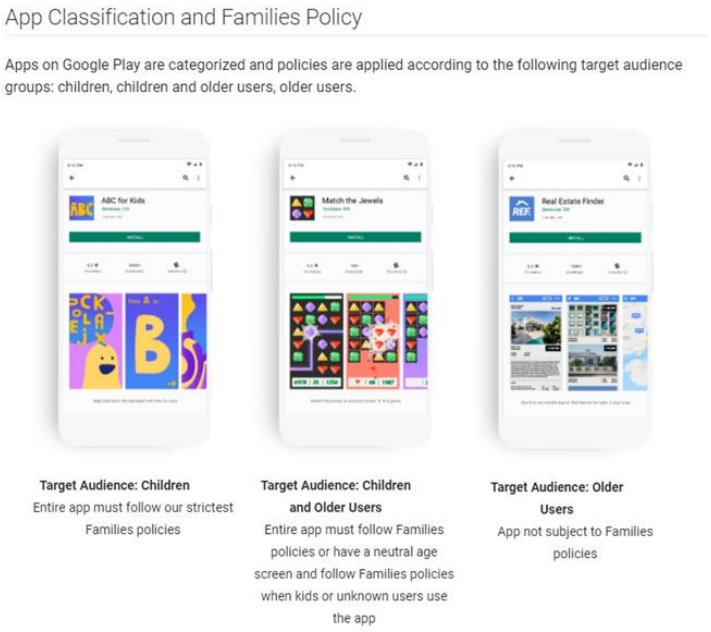

Figure 2

42. Similarly, Google offers its own content-based rubric that identifies whether an app is child-directed ("Manage target audience and app content settings"[16]), including whether apps:

- Support non-readers, or early readers, with limited reliance on text
- Have a simple design with large iconography and clear, consistent interactive elements
- Center on pretend play, and simple problem solving, and/or creative free play
- Are positive in tone or silly, and have a happy ending or clear takeaway
- Contain funny and/or popular characters or stories, even slapstick humor and hyperbole
- Utilize badges, collecting characters, unlocking levels, or other age-appropriate incentives
- Relate to early education, like language development, early literacy, and basic math
- Require logic or spatial problem solving, but not necessarily deductive reasoning and abstract thinking (which may still be too hard)

[16] Google, *Play Console Help*, https://support.google.com/googleplay/android-developer/answer/9867159?visit_id=637522057853722464-2168424342&rd=1#age-groups&zippy=%2Cage-and-under%2Cages-- (last accessed July 30, 2021).

43. As demonstrated by the images below, the Angry Birds Gaming Apps contain cartoonish, animated characters designed to appeal to children, have limited to no reliance on written text, center on pretend play and simple problem solving, are silly in tone, and are easy for a young child to play.

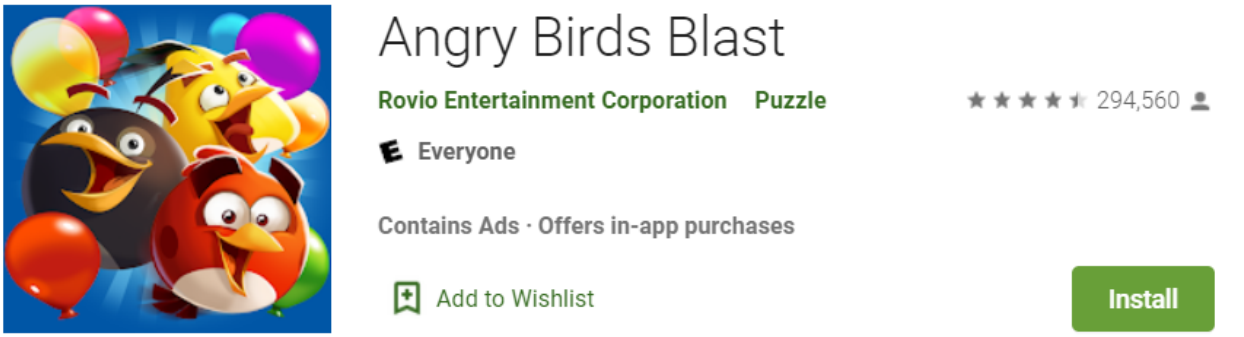

Figure 3

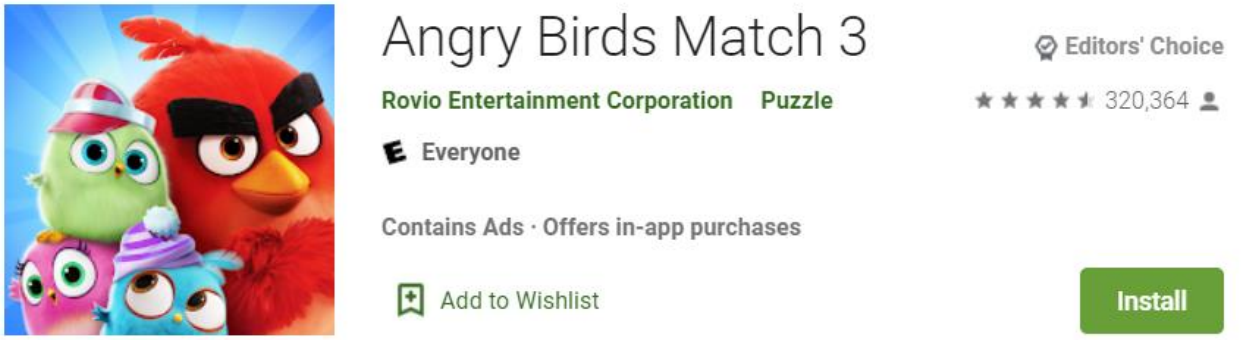

Figure 4

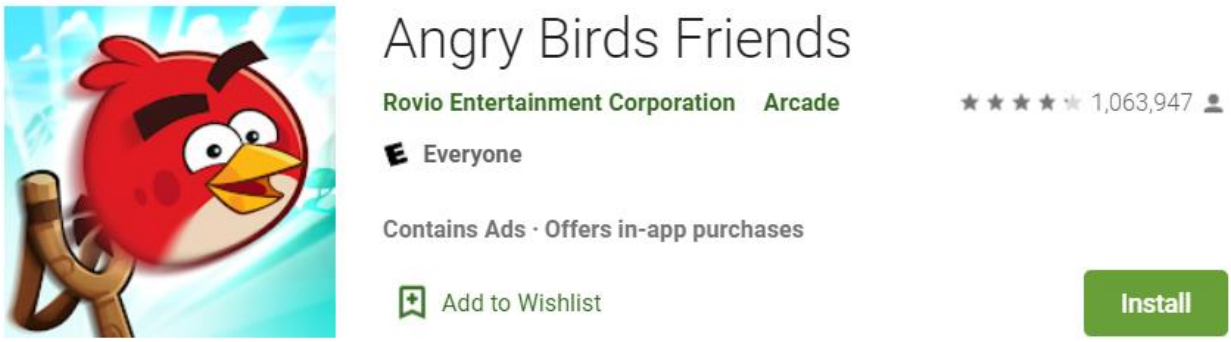

Figure 5

44. Rovio acknowledges that its Angry Birds Gaming Apps are child-directed through its decade-long, sustained campaign to market the Gaming Apps and related toys and merchandise to young children. Rovio began marketing plush toys based on the characters in the Angry Birds Gaming Apps as early as 2010. By 2012, Rovio sold tens of millions of stuffed Angry Birds toys.[17] Rovio also released a line of toys sold to children that included coupon codes providing children extra "power-ups" to enhance game play when playing an Angry Birds Gaming App, in order to encourage and induce them to purchase, download, and play the games.[18]

45. As early as 2012, Rovio focused on getting children to buy "virtual goods" (e.g., goods sold and used while playing games, like Angry Birds Rio) and actual "physical goods," like Angry Birds plush toys, children's puzzles, and coloring books. In 2012, Rovio's head of development stated that the company's goal was to create an entertainment franchise similar to Hello Kitty.[19]

46. Examples of the scores of toys and merchandise based on the cartoonish, child-directed Angry Birds characters that Rovio markets to children include baby blankets, infant Halloween costumes, action figures, children's lunchboxes, slot cars, playground equipment and playground balls:

[17] Jenna Wortham, *Angry Birds Migrates to Facebook and Toy Stres*, New York Times (February 13, 2012), https://bits.blogs.nytimes.com/2012/02/13/angry-birds-migrates-to-facebook-and-toy-stores/ (last accessed July 30, 2021).
[18] *Id*.
[19] *Id*.

Figure 6

Figure 7

Figure 8

Figure 9

Figure 10

47. Rovio currently has approximately 150 licensing arrangements, and is well aware that the cartoonish characters in its Angry Birds franchise are being used to capitalize on the Apps' huge popularity with their child audiences, in order to sell those children additional products. In each instance, Rovio approves of the product and the content, and each licensee must agree to relevant audits performed by Rovio. A sampling of fifty toys and similar Angry Birds-related merchandise targeted to children under thirteen is included in Exhibit 2.

48. In 2013, researchers with Kytephone found that the Angry Birds Gaming apps were among the most addictive apps played by kids, with Angry Birds Star Wars, Angry Birds, Bad Piggies, Angry Birds Seasons, and Angry Birds Space among the top ten most popular games calculated by how long children spent playing a particular app.[20]

[20] Sarah Perez, *Rovio Titles Among The Most Addictive Games For Kids, Study Finds*, TechCrunch, (January 21, 2013) https://techcrunch.com/2013/01/21/rovio-titles-among-the-most-addictive-games-for-kids-study-finds/ (last accessed July 30, 2021)

49. Rovio also aggressively marketed cartoons and movies intended for children, based on the characters in the Angry Birds Gaming Apps. In 2016, Rovio financed, produced and released a major animated motion picture, *The Angry Birds Movie*, through Sony Pictures Entertainment. The movie was described as "children's entertainment, [with] pleasant echoes of cartoon classics" but that ultimately "settles into the current default mode of animation humor . . . replete with bodily function jokes. The kids of today deserve better."[21] The star of the movie, Jason Sudeikis, specifically confirmed that the movie's "target audience" is children "5-10 years old."[22]

50. In 2019, Rovio and Sony released a sequel, *Angry Birds 2*, which was also directed towards children. As one reviewer noted, the movie was aimed particularly towards younger children:

> What was interesting to see was how the kids in the screening I was at reacted to the movie. The younger members of the audience lapped up the silliness and the mild peril. However, the kids at the older end of the spectrum, the ones who probably were more in the previous demographic when the first film came out, seemed entertained but less reactive and enamored by what they were seeing. The former sang along to songs on the soundtrack and repeated funny dialogue they'd just heard while the latter didn't. A few of the older kids had their phones out and generally seemed more interested in what was going on outside the theater than what was unfolding inside.[23]

---

[21] Glenn Kenny, *Review: 'The Angry Birds Movie,' a Superficially Amiable Ball of Fluff*, New York Times (May 19, 2016), https://www.nytimes.com/2016/05/20/movies/-the-angry-birds-movie-review.html (last accessed July 30, 2021).

[22] Tasneem Balapurwala, *'The Angry Birds' review: This is tailor-made for kids*, Economic Times (May 27, 2016), https://economictimes.indiatimes.com/magazines/panache/the-angry-birds-review-this-is-tailor-made-for-kids/articleshow/52460076.cms?from=mdr (last accessed July 30, 2021).

[23] Simon Thompson, *The Angry Birds 2 Movie Review: Only little kids and their parents will likely want to flock to see this sweet but derivative sequel*, IGN (August 13, 2019), https://www.ign.com/articles/2019/08/13/the-angry-birds-movie-2-review (last accessed July 30, 2021).

51. In March 2020, a spokesperson for Netflix said: "Angry Birds have been a true phenomenon for kids round the world and we're excited to bring them home to the nest at Netflix where they will be angrier and bird-ier than ever."

52. In May 2021, leading on-demand kids service Toon Googles added a special brand channel for Angry Birds.

53. Also in May 2021, Burger King collaborated with Rovio to incorporate the Angry Birds franchise into its King Jr. kids' meals—smartphone users who scan QR codes on Burger King's plush Angry Birds toy tags, box packaging and signage will activate an Angry Birds augmented reality game on their mobile device.

54. The original Angry Birds app cost $1.99 to download. Over the years, app prices ranged from $0.99 to $1.99, with the purchase of over 3 billion Angry Birds Gaming Apps.

55. Rovio also merchandises to—and monetizes—children with "in-app" purchases that allow them to buy in-game goods or services while playing the Angry Birds Gaming Apps. Prices for these in-app purchases range from $1.99 to $99.99. Examples of more than one hundred in-app purchase options and their prices are attached as Exhibit 3.

56. Rovio also sells numerous toys and other merchandise to children based on the Angry Birds Gaming Apps that include conduits for the child to download or otherwise access the apps. Examples include:

- Angry Birds Apptivity King Pig Figure Pack by Mattel – "Kids can immerse themselves in the action with these single packs that come with a touchscreen conductive base and accessory that enables consumers to use them in conjunction with the associated Angry Birds app."[24]

[24] Toywiz.com, *Angry Birds Apptivity King Pig Figure Pack by Mattel*, https://toywiz.com/angry-birds-apptivity-king-pig-figure-pack/ (last accessed July 30, 2021); *see, also,* Walmart.com https://www.walmart.com/ip/Apptivity-Angry-Birds-King-Pig-Single-Pack-by-Mattel-toy-gift-idea-birthday/495340276 (same) (last accessed (July 30, 2021)

- Angry Birds Mission Flock Pack by Jazwares touts the Angry Birds Explore Logo which allows one to "Scan With App For Preview" which "Unlocks Exclusive Game Inside."[25]
- Angry Birds Transformers Telepods: Autobird Jazz Bird vs. Deceptihog Brawl Pig by Hasbro allows one to "teleport your bird and pig into the Angry Birds Transformers app. Just put one of them on the base and put the base on your device (sold separately) and scan it into the app. Now you can play as that converting pig or bird!"[26]

57. The child-directed nature of the Angry Birds Gaming Apps is readily apparent both from the appearance and content of the apps themselves and from the exensive merchandise licensing that Rovio has done to capitalize on the apps' popularity with children. However, Rovio's own words belie Rovio's knowledge of the child-directed nature of the Gaming Apps. On its website, under a heading titled "Rovio for Parents," Rovio states:

> **Kids love playing our games!** We strive to create fun and engaging games that people of all ages can enjoy, and **we're totally jazzed that so many young kids gravitate towards our titles. Thank you parents for allowing your children to enjoy our games!**[27]

58. It is beyond dispute that Rovio knows that the primary audience for the Angry Birds Gaming Apps is children. Yet Defendant harvests children's Personal Information from the child-

---

[25] Toywiz.com, *Angry Birds Mission Flock Pack – Leonard and Red*, https://toywiz.com/angry-birds-mission-flock-pack-leonard-red-figure-2-pack/ (last accessed July 30, 2021)

[26] Amazon.com, *Hasbro, Angry Birds Transformers Telepods Autobird Jazz Bird vs. Deceptihog Brawl Pig Figure 2-Pack [Deceptihogs Revenge]*, https://www.amazon.com/Hasbro-Transformers-Telepods-Deceptihog-Deceptihogs/dp/B00TOX44K6/ (last accessed July 30, 2021)

[27] Rovio, *How Can I Stop My Child From Making In-App Purchases Without Permission?*, (2018) available at https://info.rovio.com/hc/en-us/articles/360000982888-For-Apple-iOS- (for Apple iOS devices); https://info.rovio.com/hc/en-us/articles/360000982868-For-Google-Play-Android (for Google Play Android devices); https://info.rovio.com/hc/en-us/articles/360000972707-For-Amazon-Android- (for Amazon Android devices) (last accessed July 30, 2021).

directed Angry Birds Gaming Apps in connection with: (i) children's purchase of the Angry Birds Gaming Apps; (ii) children's purchase of virtual goods within those Gaming Apps that enhance play and promote continued play; and (iii) children's play of the Angry Birds Gaming Apps themselves, which is encouraged by the marketing of related toys and merchandise.

D. Rovio's Privacy Policy Cynically and Misleadingly Ignores Facts Rovio Knows to Be True, and Claims That the Angry Birds Gaming Apps are Not Intended for the Child Audience That Rovio Actively Courts.

59. As shown above, Rovio actively markets its Angry Birds Gaming Apps and their attendant toys, shows, movies, and other paraphernalia to young children. Despite its clear public representations, Rovio cynically attempts to avoid its obligations under the law to protect the privacy of its child audience.

60. In an attempt to innoculate itself from potential liability, Rovio crafted a privacy policy for the Angry Birds Gaming Apps that expressly disavows its actual audience, stating:

> Under our Terms of Service, you represent that you are at least 13 years of age. However, we do not know the specific age of individual users of our Services. If you are under 13 years of age, please do not provide your personal data (including your name, address, telephone number, or email address) to us or use the Services to make your personal data available to others.
>
> If we discover that we hold personal data relating to a user under 13 years of age, we will take appropriate measures to ensure that we process that data according to the requirements of applicable laws and regulations or promptly delete the data from our records. If you have reason to believe we hold personal data relating to a user under 13 years of age, please contact us.[28]

61. Rather than adapting its privacy policy to the fact that "Kids love playing our games!" and "[W]e're totally jazzed that so many young kids gravitate towards our titles,"[29] thus abiding by its obligations under COPPA to protect children and respect parental autonomy, Rovio elected to go the opposite route: declaring—without any reasonable basis and contrary to all

[28] Rovio, *Privacy Policy*, at Section 11 ("Age Limit"). (January 30, 2020) https://www.rovio.com/privacy/ (last accessed July 30, 2021).
[29] *See*, fn. 26, *supra*.

public-facing representations and evidence—that anyone who plays the Angry Birds Gaming Apps is an adult, unless the child user – unprompted but for a single paragraph buried deep within a privacy policy – somehow provides unsolicited information to the contrary. As discussed immediately below, this cynical ploy is expressly prohibited under COPPA.

E. The FTC Recognizes that Sites and Services Directed to Children May Have Audiences That are Not Exclusively Children, Which Does Not Relieve Rovio of Its Obligations Under COPPA.

62. The FTC recognizes that a site or service with child-directed content may not have an audience comprised exclusively of children under the age of 13. Indeed, a site or service can be child-directed under COPPA even when children under the age of 13 are not the primary audience. In such instances, COPPA requires the developer to ensure that children under 13 do not have their Personal Information collected absent parental notice and verifiable parental consent. Per the FTC:

> [COPPA] provides a *narrow* exception for a site or service that may be directed to children under the criteria set [under the Rule], but that does not target children as its *primary* audience (sometimes referred to as "mixed audience"). If your site or service targets children under age 13, *but children under 13 are not your primary audience* (e.g., your site also targets adults or older teens), you can take advantage of this exception. You can implement an age screen; for users who indicate they are children under 13, you can ensure that you do not collect personal information from those users, or you can obtain verifiable parental consent. It is important to emphasize that the "mixed audience" category is a subset of the "directed to children" category[.][30]

63. The FTC further explains:

> An operator of a site or service meeting this standard may age-screen its users if it: (1) does not collect personal information from any visitor prior to collecting age information, and (2) prevents the collection, use, or disclosure of personal information from visitors

[30] FTC, *Complying With COPPA: Frequently Asked Questions*, at Section D.4 (Mar. 20, 2015) (Emphasis added), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0#D.%20Websites%20and%20Online%20Services (last accessed July 30, 2021).

> who identify themselves as under age 13 without first complying with the Rule's notice and parental consent provisions. See 16 C.F.R. § 312.2 (definition of "Web site or online service directed to children," paragraph (3)). Keep in mind that unlike a general audience website or service, as an operator of a website or online service directed to children, you may not block children from participating in the website or online service.[31]

64. Thus, even if Rovio contends that the Angry Birds Gaming Apps are "mixed audience"—a point the State does not concede—such an argument would be academic. Rovio has not implemented an age screen in any of the Angry Birds Gaming Apps, yet it is keenly aware that its primary audience is young children.[32] Accordingly, Rovio has no factual or legal basis to contend it has complied with COPPA by meeting the requirements of this "narrow exception" limited to child-directed services where the primary audience is not children under 13.

F. The SDKs Embedded in the Angry Birds Gaming Apps Surreptitiously Exfiltrate Children's Personal Information While They Play the Games.

65. As children play the Angry Birds Gaming Apps, the SDKs contained within the apps collect the children's Personal Information and, without the parent's knowledge or verifiable consent, exfiltrate the Personal Information to track and profile the children for targeted advertising and further commercial gain.

66. "Persistent identifiers" are the most common Personal Information that the SDKs take from children's devices and use for tracking, profiling, and targeting. These identifiers are a set of unique data points (typically numbers and letters), akin to a Social Security Number, and can link one specific individual to all of the apps on her device and her activity on those apps, allowing her to be tracked over time, across different app sessions, and across devices (*e.g.*, smart phones, tablets, laptops, desktops and smart TVs).

---

[31] *Id.*

[32] *See*, Exhibit 7 (Rovio states that "56% of 4-16 year olds in the US watch the Angry Birds animated series at least once or a few times a week (with 45% of kids aged 4-7 and 52% of kids aged 8-11 watching every day in the US!").

67. The common persistent identifiers in the Android operating system are the Android Advertising ID ("AAID") and the Android ID. Both the AAID and Android ID are unique, alphanumeric strings assigned to an individual device—and the individual who uses that device—in order to track and profile the user, and to serve them with targeted advertising.[33]

68. A device's International Mobile Equipment Identity ("IMEI") is also a persistent identifier. An IMEI is a fixed, unique 15-digit serial number that is used to route calls to one's phone and reflects information about the origin, model, and serial number of the device. A device has one fixed IMEI.

69. Additionally, each device can be identified by its "Device Fingerprint" data, which is another form of persistent identifier. Device Fingerprint data include myriad individual pieces of data about a specific device, including details about its hardware—such as the device's brand (*e.g.*, Apple or Android), the type of device (*e.g.*, iPhone, Galaxy, iPad)—and details about its software, such as its operating system (*e.g.*, iOS or Android). This data can also include more detailed information, such as the network carrier (*e.g.*, Sprint, T-Mobile, AT&T), whether the device is connected to Wi-Fi, and the "name" of the device. The name of the device is often particularly personal, as the default device name may be configured to include children's first and/or last names (*e.g.*, "Jane Minor's iPhone"). In combination, the pieces of data comprising the Device Fingerprint provide a level of detail about the given device that allows that device and its user to be identified individually, uniquely, and persistently—as the appellation "Fingerprint" implies.

[33] The common persistent identifiers for Apple are the ID for Advertisers ("IDFA") and ID for Vendors ("IDFV"). Both the IDFA and the IDFV are unique, alphanumeric strings that are used to identify an individual device—and the individual who uses that device—in order to track and profile the user, and to serve them with targeted advertising. However, the focus of this action is Defendant's behavior in the Android/Google marketplace, not in the Apple/iTunes marketplace. All of the Angry Birds Gaming Apps at issue in this Complaint are offered for Android devices.

70. The advertising SDKs contained within the Angry Birds Gaming Apps exfiltrate and analyze persistent identifiers, such as those described above,[34] to track children over time and across apps, devices, and websites. This is a function of a concerted and constant effort to learn more about children, including their behaviors, demographics, and preferences, and, thereafter, to serve them with tailored and targeted advertising. The advertising SDKs also use persistent identifiers to track the effectiveness of those advertisements after the child sees them (to determine, for example, whether the child downloaded the app or bought the product advertised).

71. The surreptitious exfiltration takes place as such. As soon as a New Mexico child opens up an Angry Birds Gaming App on her device and it connects to the Internet, the app will connect to servers used by the advertising SDK and other advertising companies and begin sending those servers data. This activity is invisible to the child (and her parent), who simply sees the given app's game interface.

72. Each of the advertising SDKs behaves similarly.

73. As the child plays the Angry Birds Gaming App, the embedded SDK continues to communicate with its own and other advertising companies' respective servers, sending requests for an ad—or "calls"—to those servers. With each call, the SDK also sends the child's Personal Information, including persistent identifiers.

74. The calls can serve one of two functions. First (and most common), the call is a traditional ad request, which is fulfilled by the SDK in its ad network capacity (described in the immediately-following paragraphs). Second, the SDK can provide "mediation," in which it serves as an intermediary between other, competing ad SDKs in the app, instantaneously negotiating between each SDK's unique ad network to find the highest bidder to place an ad in the app. When an SDK provides mediation services, this may result in that SDK's own ad network "winning" the

[34] There are multiple, additional items of data that are universally recognized as persistent identifiers. For example, a device's Wi-Fi MAC address is a fixed serial number used to identify one's phone when transmitting and receiving data using Wi-Fi.

bid (i.e., paying the highest price to place an ad in the Angry Birds app), or else another ad SDK might win the bid. Regardless, in its mediation capacity, an SDK is still responsible for acquiring the child's Personal Information and passing it on to the winning ad network.

75. Once exfiltrated to the SDK's servers, the Personal Information harvested from children playing the Angry Birds Gaming Apps can be combined with other data associated with those same children via the same persistent identifiers or other data (*e.g.*, online activity or demographics) which can track and individually identify the children. This is often accomplished through vast quantities of data obtained by "ad networks."

76. An ad network is also where advertising space is bought and sold. In this virtual marketplace, app developers and advertisers buy and sell advertising space and the ads to fill it. These networks connect advertisers looking to sell data-driven, targeted ads to mobile apps that want to host advertisements. A key function of an ad network is aggregating available ad space from developers and matching it with advertisers' demands.

77. Once the ad call is facilitated by the SDK, and the ad is placed on the child's device, advertising companies then store and analyze the Personal Information to enable continued tracking of the child. This further analysis and profiling includes storing information such as what ads they have already seen, what actions they took in response to those ads, other online behavior, and additional demographic data. This way, the advertising companies that design and maintain the SDK (and other affiliated entities) can generally monitor, profile, and track them over time, across devices, and across the Internet. Targeted advertising is driven by individuals' Personal Information and employs sophisticated algorithms that interpret the Personal Information to determine the most effective advertising for those individuals.[35]

78. This entire ecosystem collects and uses children's Personal Information without first providing direct parental notice *or* obtaining verifiable parental consent. This includes the

[35] For a detailed discussion of targeted advertising, see Section IV.F.1, *infra.*

companies that have SDKs embedded in the Angry Birds Gaming Apps, who fail to reasonably and meaningfully inform parents that, as children play the Angry Birds Gaming Apps, the SDKs surreptitiously collects their Personal Information and track online behavior to profile children for targeted advertising. Further, parents are not asked to consent to these practices. This is all the more egregious given that COPPA does not just require *notice* in its compliance regime, but also requires equally-critical verifiable parental consent.

G. On Rovio's Behalf, Multiple SDKs Exfiltrate Children's Personal Information While They Play at Least Eight of Rovio's Most Popular Angry Birds Gaming Apps.

79. To show ads to children via the Angry Birds Gaming Apps (through its ad network or its mediation services), an SDK embedded in the Angry Birds Gaming Apps communicates with or "makes a call" to servers used by the advertising company that develops and maintains the given SDK. For example, for the AdColony SDK—which is found in all of the Angry Birds Gaming Apps—data might be sent to servers affiliated with AdColony's web address ads30.adcolony.com. The call would then request that an ad be shown to a particular child while he or she is playing the game.

80. Through this call, the given SDK receives the child's Personal Information, in the form of persistent identifiers including, among others, the child's AAID.

81. The SDK also receives the IP address of the child's device, which enables the identification of the child's location, the identification of the child's device, and cross-device tracking.

82. The SDK's call to its servers also discloses other valuable Personal Information in the form of Device Fingerprint data that can be used to identify, profile, and target specific children. This information can include, *inter alia*:

a. the manufacturer, make, and model of the child's device;

b. the operating system of the child's device; and

c. the name and developer of the app the child is operating.

Data Point	Exemplar Data Field[36]	Personal Information Derived from Data
AAID	A42c89c4-1dc7-5b79-92cd-01fa2cd5cab2	Jane Minor's device's unique AAID
Child's device's IP address	206.3.128.12	Jane Minor's device can be identified and located on the Internet, her location can be identified, and she can be tracked across devices via this number
Manufacturer, make, and model of the child's device	SAMSUNG-SM-G935A Build/R16NW	Jane Minor is playing Angry Birds 2 on her Samsung Galaxy Model No. G935A, Build Number R16NW, on the Android OS
Child's device operating system and version	User-Agent: Android 8.0.0	Jane Minor's phone is running the Android operating system, version 8.0.0
Application name and developer	App: com.rovio.baba	Jane Minor is an Angry Birds 2 user

83. With only minor, immaterial variations, each SDK behaves similarly in each of the Angry Birds Gaming Apps in which it is embedded—surreptitiously exfiltrating children's Personal Information (including but not limited to persistent identifiers), without verifiable parental consent.

84. As alleged herein, each SDK identified as being embedded in the Angry Birds App is in the business of collecting Personal Information to track and profile children and sharing such Personal Information with publishers, advertisers, service providers, and other affiliates.

85. Rovio's and the SDKs' concerted efforts to exfiltrate children's Personal Information—for purposes of tracking and profiling children—are undertaken without (1) reasonable and meaningful direct notice to parents, or (2) verifiable parental consent.

[36] The figures in this table are exemplars and do not disclose any individual's personally identifying information. Except where indicated otherwise, these exemplar data points are in the context of the gaming app Angry Birds 2 on an Android device.

H. Rovio Contracts with Numerous SDKs to Exfiltrate Children's Personal Information for the Purpose of Commercial Exploitation.

86. Since the introduction of the Angry Birds Gaming Apps in 2009 up until the present, Rovio has partnered with numerous advertising technology companies, embedding their SDKs into the Angry Birds Gaming Apps to exfiltrate children's Personal Information for the purpose of tracking them over time and across the internet for psychological and commercial exploitation.

87. These advertising partners with whom Rovio has partnered to show third-party ads in Angry Birds Gaming Apps include, but are not limited to, the following: AdColony, Adjust, AdMob (Google's advertising SDK), Amazon, Apex Mobile Media, Applifier, District M, Etermax, Facebook, Gameloft, IAB, ironSource, Lifestreet, Liftoff, LoopMe, Magnite, Moat/Oracle, My.com, PubMatic, Smartclip, Smartstream.tv, SpotX, TikTok, Tremor, Unity, Venatus Media, Verve, Vungle, and Zendesk (collectively, the "Advertising Partners").

88. These Advertising Partners actively courted Rovio to place their SDKs within the Angry Birds Gaming Apps. In so doing, they acquired actual knowledge that the apps are child-directed. As one example, in a 2015 blog post describing the launch of Angry Birds 2, AdColony praises the app as follows:

> **Users Flock to Angry Birds 2**
> Rovio still has the magic touch: over a million users installed their latest title Angry Birds 2 within the first 12 hours of its launch. Originally launched in 2009, the Angry Birds franchise has enjoyed numerous spinoffs and product launches, from plushies to bird shaped candy.
>
> The new version of the game adds new spells, levels, birds, and opportunities for in-app purchases.
>
> As Rovio has already proven successful at turning their game into an entertainment brand, it will be most interesting to see the impact

> the new game has on their franchise and how they are able to drive even stronger user retention and LTV.[37]

89. Additional Advertising Partners make similar representations and have a similar level of awareness not only of the Angry Birds Gaming Apps themselves, but of Rovio's broader footprint in the entertainment industry and the child-directed nature of its related toys, children's merchandise, animated shows, and movies.

90. On information and belief, each of the Advertising Partners: (a) has actual knowledge that the Angry Birds Gaming Apps are child-directed; (b) has actual knowledge of the child-directed nature of the related toys, children's merchandise, animated shows, and movies that are based on the Angry Birds Gaming Apps and targeted to the same audience; (c) has actual knowledge that they collect and/or receive personal information of users of the Angry Birds Gaming Apps either directly from the Angry Birds Gaming Apps or from Rovio; (d) negotiated and executed a contract with Rovio to harvest personal information from the Angry Birds Gaming Apps for the purpose of targeted, non-contextual advertising; (e) has an account manager or similar employee who tracks and cultivates the partnership with Rovio; and (f) closely tracks the revenue it generates from the monetization of personal information harvested from the Angry Birds Gaming Apps.

91. As examples, six of the Advertising Partners are highlighted below.

92. **Facebook:** Facebook is one of the largest data aggregators in the world. Facebook's popularity hinges upon the ability of its users to communicate with one another. As the company stated in a Securities and Exchange Commission filing in anticipation of its May 2013 initial public offering "[p]eople use Facebook to stay connected with their friends and family, to discover what is going on in the world around them, and to share and express what matters to them to the people they care about . . . . We believe that we are at the forefront of enabling faster, easier, and richer

[37] AdColony, *Mobile Monday: Automated Evolution, Mobcrush & More Angry Birds* (Aug. 3, 2015) https://www.adcolony.com/blog/tag/rovio/ (last accessed July 30, 2021).

communication between people and that Facebook has become an integral part of many of our users' daily lives."[38] Since its inception, Facebook continuously has been scrutinized by regulators for its abusive data-handling practices, including with regard to children's data.[39] Facebook's practices regarding Rovio are no different: the company has entered into bespoke contracts with Rovio regarding its Angry Birds Gaming Apps and beyond.[40] Per Facebook, "Rovio was one of the earliest adopters of app bidding and began testing app bidding with Facebook Audience Network in 2017. Both Rovio and Audience Network shared a vision to create a more fair and open ad ecosystem, which was a key reason Rovio chose to partner with Audience Network."[41] Facebook was well aware of each and every facet of Rovio's business (including the child-directed nature of same), describing its familiarity not just with "the global Angry Birds brand, which started as a popular mobile game in 2009," but also Rovio's subsequent "evol[ution] from games to various entertainment and consumer products in brand licensing."[42] Indeed, Facebook's SDK is found in each of the Angry Birds Gaming Apps.

93. Facebook is in the business of collecting personal information to track and profile users—including children—and sharing that personal information with publishers, advertisers, service providers, and Facebook affiliates. Rovio engages Facebook to perform these same services. Rovio and Facebook do not provide parents the disclosures and notice required by

---

[38] Form S-1 Registration Statement for Facebook, Inc., as filed with the Securities and Exchange Commission, "Prospectus Summary," at 1 (Feb. 1, 2012), http://www.sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm (last accessed July 30, 2021).

[39] *See, e.g.*, FTC, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019) https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions (last accessed July 30, 2021).

[40] *See, e.g.*, Facebook Audience Network Blog, *Rovio moves more than 90% of inventory to app bidding after seeing positive impact on ad revenue and operational efficiency* (June 24, 2019) https://www.facebook.com/audiencenetwork/resources/success-stories/rovio (last accessed July 30, 2021).

[41] *Id*.

[42] *Id*.

COPPA nor do they obtain verified parental consent prior to harvesting children's personal information through Facebook's SDK.

94. **AdColony:** AdColony is a "mobile video ad network and monetization solution."[43] As an ad network, AdColony works with both app developers and brands seeking to place video ads on apps to generate revenue through this advertising.[44] AdColony claims it will connect advertisers to "top trending mobile environments where consumer attention lives" using a "combination of data, tech [and] creativity."[45] As for app developers like Rovio, AdColony states that it will provide access to the "world's top mobile publishers" to fill their ad space, including through a variety of video ads.[46] AdColony also facilitates rewarded video ads, wherein users "watch a video ad and are rewarded with virtual currency."[47] Often, app developers are both developers and advertisers: they want to fill ad space in their apps, but also advertise their app in other mobile apps.[48] AdColony offers a platform for them to do so. AdColony's SDK has been embedded in more than 200 apps, and downloaded more than 40 million times.[49] It reaches an estimated 1.4 billion users.[50]

95. AdColony is in the business of collecting personal information to track and profile users—including children—and sharing that personal information with publishers, advertisers,

[43] "About AdColony," AdColony, http://support.adcolony.com/customer/en/portal/articles/313633-about-adcolony (last accessed July 30, 2021).
[44] *Id.*
[45] "Highest Quality Mobile Experiences: Reaching an Audience of 1.4 Billion Engaged Mobile Users," AdColony, https://www.adcolony.com/advertisers/ (last accessed July 30, 2021).
[46] "Grow With Us - Maximizing App Economies for Today's Top Mobile Publishers," AdColony, https://www.adcolony.com/publishers/ (last accessed July 30, 2021).
[47] "About AdColony," AdColony, http://support.adcolony.com/customer/en/portal/articles/313633-about-adcolony (last accessed July 30, 2021).
[48] *Id.*
[49] *Id.*
[50] "Highest Quality Mobile Experiences - Reaching an Audience of 1.4 Billion Engaged Mobile Users," AdColony, https://www.adcolony.com/advertisers/ (last accessed July 30, 2021).

service providers, and AdColony affiliates. Rovio engages AdColony to perform these same services. Rovio and AdColony do not provide parents the disclosures and notice required by COPPA nor do they obtain verified parental consent prior to harvesting children's personal information through AdColony's SDK.

96. **Flurry:** Flurry is a mobile and analytics advertising company working with more than 250,000 developers and one million apps that provides "various services to build, measure, advertise, and monetize various applications."[51] Flurry claims to "[h]elp developers and marketers measure and analyze their applications in order to grow, retain, and monetize their users."[52] This includes helping developers "target [their] users" using "demographic information" and their app use, among other data points.[53]

97. Flurry is in the business of collecting personal information to track and profile users—including children—and sharing that personal information with publishers, advertisers, service providers, and Flurry affiliates. Rovio engages Flurry to perform these same services. Rovio and Flurry do not provide parents the disclosures and notice required by COPPA nor do they obtain verified parental consent prior to harvesting children's personal information through Flurry's SDK.

98. **ironSource:** ironSource is a mobile advertising company that helps developers "turn their digital content into viable businesses without having to charge for them."[54] In other words, it helps developers who want to offer free apps make money through advertising revenue. ironSource does this by using data to target potential app customers (it calls this "multi-touchpoint

---

[51] "Company Overview of Flurry, Inc.," Bloomberg, https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=25475459 (last accessed July 30, 2021).

[52] "Oath is Home to the Media, Tech, and Communication Brands That 1 Billion People Love and Trust. Explore Them All Here," Oath, https://www.oath.com/our-brands/ (last accessed June 4, 2018).

[53] "Flurry Push," Flurry, http://www.flurry.com/push.html (last accessed July 30, 2021).

[54] "We're all-in Players," ironSource, https://www.ironsrc.com/about/ (last accessed July 30, 2021).

data targeting") and by providing ads for placement inside the app, telling developers it can provide "every kind of ad out there to make sure [they] can pull from the widest possible range and build the right experience for each user."

99. ironSource is in the business of collecting personal information to track and profile users—including children—and sharing that personal information with publishers, advertisers, service providers, and ironSource affiliates. Rovio engages ironSource to perform these same services. Rovio and ironSource do not provide parents the disclosures and notice required by COPPA nor do they obtain verified parental consent prior to harvesting children's personal information through ironSource's SDK.

100. **Unity:** Unity is a mobile advertising company. Unity markets its ability to increase user engagement with mobile apps and deliver profitable targeted advertisements. As it states on its website, "Unity Ads enables publishers to integrate video ads into [their] mobile games in a way that both increases player engagement and puts more money in [developer's] pocket over the gamer's lifetime."[55] Unity's technology is widely used in the mobile gaming industry and it claims its "engine is far more popular amongst developers than any other third-party game development software."[56] Using Unity's technology, app developers can, as Unity represents, "[b]e among the first to access . . . a whole network of advertisers competing for space in your game - and paying top dollar."[57] Unity's SDK technology collects user information for purposes of serving targeted advertisements: "Machine Learning Based Targeting delivers to advertisers the most relevant eyeballs."[58]

---

[55] "Unity Ads: Get Paid for All Your Hard Work," Unity, https://unity3d.com/unity/features/ads (last accessed July 30, 2021).
[56] "Unity: Company Facts," Unity, https://unity3d.com/public-relations (last accessed July 30, 2021).
[57] "Unity Ads: Get Paid for All Your Hard Work," Unity, https://unity3d.com/unity/features/ads (accessed July 30, 2021).
[58] *Id.*

101. Unity is in the business of collecting personal information to track and profile users—including children—and sharing that personal information with publishers, advertisers, service providers, and Unity affiliates. Rovio engages Unity to perform these same services. Rovio and Unity do not provide parents the disclosures and notice required by COPPA nor do they obtain verified parental consent prior to harvesting children's personal information through Unity's SDK.

102. **Vungle:** Vungle is a mobile advertising company that claims to "deliver the highest value users through engaging video ads" to its clients—more than 50,000 mobile apps worldwide—to help them maximize profits by delivering targeted ads: "Advertisers depend on Vungle's creative optimization technology, targeting and HD video ad delivery to reach and acquire high-quality users worldwide."[59] On its website, Vungle offers advertisers its SDK technology and markets its ability to "reach more valuable mobile consumers" by targeting consumers based on, among other information, "device type, settings, app, language, country, city and much more."[60]

103. Vungle is in the business of collecting personal information to track and profile users—including children—and sharing that personal information with publishers, advertisers, service providers, and Vungle affiliates. Rovio engages Vungle to perform these same services. Rovio and Vungle do not provide parents the disclosures and notice required by COPPA nor does they obtain verified parental consent prior to harvesting children's personal information through Vungle's SDK.

[59] "About Us," Vungle, https://vungle.com/about/ (last accessed July 30, 2021).

[60] "Reach More Valuable Mobile Consumers," Vungle, https://vungle.com/user-acquisition/ (last accessed on July 30, 2021).

I. The Privacy-Invasive and Manipulative Commercial Purposes Behind Defendant's Data Exfiltration, and its Effect on Children

1. The Role of Personal Information in User Profiling and Targeted Advertising.

104. Rovio and the Advertising Partners, in coordination, collect and use the Personal Information described above to track, profile, and target children with targeted advertising.

105. As noted above, when children are tracked over time and across the Internet, various activities are linked to a unique and persistent identifier to construct a profile of the child using a given mobile device. Viewed in isolation, a persistent identifier is merely a string of numbers uniquely identifying a child, but when linked to other data points about the same child, such as app usage, geographic location (including likely domicile), and Internet navigation, it discloses a personal profile that can be exploited in a commercial context.

106. But Rovio and its partners aggregate this data, and also buy it from and sell it to other third parties, all the while amassing more data points on children to build ever-expanding profiles for enhanced targeting. Across the burgeoning online advertising ecosystem—often referred to as the "mobile digital marketplace"—multiple ad networks or other third parties can buy and sell data, exchanging databases amongst themselves, creating an increasingly sophisticated profile of how, when, and why a child uses her mobile device, along with all of the demographic and psychographic inferences that can be drawn therefrom.

107. The FTC expressed "[c]oncerns about creations of detailed profiles based on device IDs [such as those created and facilitated by Defendant]…where…companies (like ad networks and analytics providers) collect IDs and other user information through a vast network of mobile apps. This practice can allow information gleaned about a user through one app to be linked to information gleaned about the same user through other apps."[61]

[61] Federal Trade Commission, "Mobile Apps for Kids: Disclosures Still Not Making the Grade." FTC Staff Report (Dec. 2012), at 9.

108. Rovio and its Advertising Partners traffic in the same data identified by the FTC (persistent identifiers such as AAID and Device Fingerprint data) causing the same harm identified by the FTC: allowing ad networks to combine data points about children from a multitude of apps.

109. The FTC Mobile Apps for Kids Report cautions that it is standard practice—and long has been standard practice—for ad networks, mobile advertisers, and ad middlemen (including, for example, Rovio, its Advertising Partners, and their partners and agents) to link the persistent identifiers they acquire with *additional* Personal Information—such as name, address, and email address—allowing those entities and their partners to identify individual users whom they profile with indisputably individual specificity.[62]

110. Indeed, key digital privacy and consumer groups have described why and how a persistent identifier alone facilitates targeted advertising, effectively rendering meaningless any claims of "anonymized" identifiers:

> With the increasing use of new tracking and targeting techniques, any meaningful distinctions between personal and so-called non-personal information have disappeared. This is particularly the case with the proliferation of personal digital devices such as smart phones and Internet-enabled game consoles, which are increasingly associated with individual users, rather than families. This means that marketers do not need to know the name, address, or email of a user in order to identify, target and contact that particular user.[63]

[62] Federal Trade Commission, "Mobile Apps for Kids: Disclosures Still Not Making the Grade." FTC Staff Report (Dec. 2012), at 10 n. 25 (citing Jennifer Valentino-DeVries, *Privacy Risk Found on Cellphone Games, Digits Blog*, Wall St. J. (Sept. 19, 2011), http://blogs.wsj.com/digits/2011/09/19/privacy-risk-found-on-cellphone-games/ (noting how app developers and mobile ad networks often use device IDs to keep track of user accounts and store them along with more sensitive information like name, location, e-mail address or social-networking data) (last accessed July 30, 2021).

[63] Comments of The Center for Digital Democracy, et al., FTC, *In the Matter of Children's Online Privacy Protection Rule* at 13-14 (Dec. 23, 2011).

111. A 2012 chart of the mobile digital marketplace,[64] attached hereto as Exhibit 4, indicates that hundreds of intermediaries from location trackers to data aggregators to ad networks "touch" the data that is used to track and profile an individual in a given online transaction.

112. By 2017, the number of unique companies in this space swelled to almost 5,000, as shown in Exhibit 5, attached hereto.[65]

113. In the course of disclosing Personal Information to select and serve an advertisement (or to conduct any third-party analytics or otherwise monetize user data), the developer and its partner SDKs pass identifying user data to an ever-increasing host of third-parties, who, in turn, may pass along that same data to *their* affiliates. Each entity may use that data to track users over time and across the Internet, on a multitude of increasingly complex online pathways, with the shared goal of targeting users with advertisements.

114. The ability to serve targeted advertisements to (or to otherwise profile) a specific user no longer turns upon obtaining the kinds of data with which most consumers are familiar (name, email addresses, etc.), but instead on the surreptitious collection of persistent identifiers or geolocation, which are used in conjunction with other data points to build robust online profiles. These data points are better tracking tools than traditional identifiers because they are unique to each individual, making them more akin to a Social Security Number. Once such uniquely identifiable data are sent "into the marketplace," they are exposed to—and thereafter may be collected and used by—an almost innumerable set of third parties.

115. Permitting technology companies to obtain children's Personal Information exposes those children to targeted advertising. The ad networks, informed by the surreptitious

---

[64] Laura Stampler, "This RIDICULOUS Graphic Shows How Messy Mobile Marketing Is Right Now," Business Insider (May 23, 2012), http://www.businessinsider.com/this-ridiculous-graphic-shows-how-the-insanely-complicated-world-of-mobile-marketing-works-2012-5 (last accessed July 30, 2021).

[65] Scott Brinker, "Marketing Technology Landscape Supergraphic" Chief Marketing Technology Blog (May 10, 2017), https://chiefmartec.com/2017/05/marketing-techniology-landscape-supergraphic-2017/ (last accessed July 30, 2021).

collection of Personal Information from children, will assist in the sale of advertising placed within the Angry Birds Gaming Apps and targeted specifically to children.

116. As established above, Rovio and its Advertising Partners exfiltrate children's Personal Information or other information about their online behavior, which is then sold to third parties who track multiple data points associated with those children, analyzed with sophisticated algorithms to create a user profile, and then used to serve targeted advertising to children whose profiles fit a set of demographic and behavioral traits.

2. Rovio and Its Advertising Partners Use Children's Personal Information to Target Them, Despite Children's Heightened Vulnerability to Advertising.

117. Rovio and its Advertising Partners use children's Personal Information to serve them targeted advertising. They engage in this illegal behavior despite the known risks associated with and ethical norms surrounding advertising to children.[66]

118. Advertisers regard children to be valuable advertising targets.[67] Children influence the buying patterns of their families—an influence that amounts to billions of dollars each year—and have lucrative spending power themselves.[68] Children and teens are thus prime targets for advertisers.

---

[66] Kristien Daems, Patrick De Pelsmacker & Ingrid Moons, *Advertisers' perceptions regarding the ethical appropriateness of new advertising formats aimed at minors*, J. of Marketing Communications (2017) at 13 ("In general, all advertising professionals acknowledge that children are a vulnerable advertising target group.").

[67] Lara Spiteri Cornish, *'Mum, can I play on the Internet?' Parents' understanding, perception, and responses to online advertising designed for children*, 33 Int'l J. Advertising 437, 438 (2014) ("Indeed, in recent years, marketers targeting children have developed a strong online presence . . ."); Issie Lapowsky, "Why Teens are the Most Elusive and Valuable Customers in Tech," Inc., https://www.inc.com/issie-lapowsky/inside-massive-tech-land-grab-teenagers.html (accessed on July 30, 2021).

[68] Sandra L. Calvert, *Children as Consumers: Advertising and Marketing*, 18 Future Child 205, 207 (2008).

119. Rovio intentionally profits from embedding advertising SDKs, to collect and exploit children's Personal Information into its Angry Birds Gaming Apps.

120. Rovio targets advertising efforts at children despite widespread awareness that children are more vulnerable to deception by advertisers because they are easily influenced by its content, lack the cognitive skills to understand the intention of advertisers, and can struggle to distinguish between advertisements and other content.[69] This is particularly problematic when targeted advertising is used because it is designed to more effectively sway target audiences.[70]

121. Exposure to advertising can also lead to negative outcomes for children, including increasing conflict with their parents, cynicism, health issues, and increased materialism.[71]

122. Children often lack the skills and knowledge necessary to assess and appreciate the risks associated with online data exfiltration and tracking.[72] Even attempts to disclose privacy-violative behavior are not easily understood. Research has found that policies explaining the exfiltration and use of children's data are difficult even for adults to understand, and marketers make no effort to explain their targeted marketing practices to child and teen audiences in developmentally appropriate and easy-to-understand ways.[73] This practice "could mislead these vulnerable emerging consumers into thinking that they are only playing games and their data are not collected for any purpose."[74]

---

[69] *Online Advertising on Popular Children's Websites: Structural Features and Privacy Issues*, *infra* at 74, at 1510 (collecting studies); *Children as Consumers: Advertising and Marketing*, *supra* at 56; *Advertisers' perceptions regarding the ethical appropriateness of new advertising formats aimed at minors*, *infra* at 54, at 2 (collecting studies); *'Mum, can I play on the internet?'*, *supra* at 55, at 438-39 (collecting studies).

[70] Olesya Venger, *Internet Research in Online Environments for Children: Readability of Privacy and Terms of Use Policies; The Uses of (Non)Personal Data by Online Environments and Third-Party Advertisers*, 10 Journal of Virtual Worlds Research 1, 8 (2017).

[71] *Children as Consumers: Advertising and Marketing*, *supra* at 56, at 118-119.

[72] Ilene R. Berson & Michael J. Berson, *Children and their Digital Dossiers: Lessons in Privacy Rights in the Digital Age*, 21 Int'l J. of Social Education 135 (2006).

[73] *Internet Research in Online Environments for Children*, *supra* at 58, at 9.

[74] *Internet Research in Online Environments for Children*, *supra* at 58, at 10.

3. Rovio and Its Advertising Partners Exfiltrate and Analyze Children's Personal Information to Track the Effect of Their Ads on Children's Behavior.

123. In the Angry Birds Gaming Apps, children's Personal Information is exfiltrated and analyzed before and after serving advertisements. On the front end, the data helps Rovio and its Advertising Partners know what ads to serve (based on children's demographics and behaviors). On the back end, the data helps them determine whether the ad succeeded in affecting children's behavior, a practice known as ad attribution.

124. These entities track the impact and value of the ads served by tracking children's activities across the Internet after they interact with those ads.

125. Rovio and its Advertising Partners want to reward advertisers whose ads influenced children's behavior. But such attribution requires surveillance. For example, if 10-year-old Sally is served an ad for a pony game based on her age, implied income, and online activities, and later goes and downloads that pony game, the advertiser responsible for the pony game ad wants that download attributed to them, so that they can get paid for that action. But the only way for the advertising companies to connect the Sally that saw the ad with the Sally that downloaded the app is to track Sally's online activities after she was shown the ad through the app—such as by tracking her persistent identifiers.

126. This ongoing exfiltration, tracking, and analysis violates children's privacy and exploit their vulnerabilities.

4. Rovio and its Advertising Partners Use Personal Information to Encourage Children to Continue Using the Angry Birds Gaming Apps, Increasing the Risks Associated with Heightened Mobile Device Usage.

127. Rovio and its Advertising Partners, and the host of other third-party advertisers to whom Defendant makes children's Personal Information available, benefit from increased mobile device usage among children. The longer and more often a child plays Rovio's games, the more Personal Information about that child the SDKs can exfiltrate and commercialize. This increased

opportunity to exfiltrate and monetize children's Personal Information and expose them to advertising is critically important to Rovio and its Advertising Partners.[75]

128. The mobile advertising ecosystem actively feeds increases in app use and mobile device addiction. Rovio and its Advertising Partners use Personal Information to program their apps to "hook" children, and to keep them playing the app.[76]

129. A key service promoted by the SDKs to Rovio and others is its ability to help apps retain their users, *i.e.*, to keep children playing their apps and thereby increase their profits. Children are specifically targeted as part of this goal.

130. These retention services are fueled by children's Personal Information. To enhance retention, the SDKs use children's Personal Information to analyze their demographics and behavior, and trigger events—both within the app and across the Internet—that will encourage them to play any app more often and for longer periods.

131. The SDKs exfiltrate children's Personal Information from their devices and use it for tracking and targeting to entice the children to play the Angry Birds Gaming Apps longer and more often. The SDKs use sophisticated algorithms to determine whether and when to target children with specific in-app cues or out-of-app ads. This behavior increases the revenue of Rovio and its Advertising Partners, all the while violating children's privacy and exposing them to the negative outcomes associated with increased mobile device usage by children.

132. These "retention" efforts take place in a context where mobile device usage among children is widespread and growing. As of 2020, 97% of families with children younger than 8-years-old had a smartphone, and 75% had a tablet.[77] The proportion of homes with a tablet has

---

[76] "Brain Hacking," *infra* at 82; Glow Kids, *infra* at 80, at XVIII-XIX, 22, 32.

[77] The Common Sense Census: Media Use By Kids Age Zero To Eight, Common Sense Media (2020), https://www.commonsensemedia.org/sites/default/files/uploads/research/2020_zero_to_eight_census_final_web.pdf (accessed on July 30, 2021).

nearly doubled since 2013.[78] Often, children have their own devices; as of 2020, 48% of children younger than 8-years-old had their own mobile device, up from only 3% in 2011 and 12% in 2013.[79]

133. Children spend increasingly more time on mobile devices. On average, a child younger than 8-years-old spends 55 minutes every day on a mobile device, nearly four times the average time spent in 2013,[80] while children between the ages of eight and twelve spend 141 minutes on mobile devices and teens spend 252 minutes.[81] Mobile games are popular among children, second only to watching TV or videos.[82] Children younger than 8-years-old spend an average of 13 minutes every day gaming, more than doubling since 2013.[83] 27% of children ages 8 to 18 report playing mobile games every day,[84] and those who play games average about 80 minutes every day doing so.[85]

134. As the use of mobile devices rises, so too do awareness of and concern about the effects of this use on children.[86] The consequences of mobile device overuse, particularly among

---

[78] *Id.*

[79] *Id.*

[80] *Id.* at 25

[81] Victoria Rideout, "The Common Sense Census: Media Use by Tweens and Teens," Common Sense Media (2019) at 21 https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens (accessed on July 30, 2021).

[82] Media Use By Kids Age Zero To Eight, *supra* at n.65, at 18.

[83] *Id.* at 25.

[84] Media Use by Tweens and Teens, *supra* at n.69, at 17.

[85] *Id.* at 15.

[86] *See, e.g.*, Xiaomei Cai and Xiaoquan Zhao, Online Advertising on Popular Children's Websites: Structural Features and Privacy Issues, 29 Computers in Human Behavior 1510-1518 (2013); Barry Rosenstein and Anne Sheehan, "Open letter from JANA Partners and CALSTRS to Apple Inc.," Jan. 6, 2018, https://thinkdifferentlyaboutkids.com/index.php?acc=1 (last accessed July 30, 2021) (letter to Apple citing "growing body of evidence" that increasing mobile device use leads to "unintentional negative consequences" for young users).

children, is well-known in the tech industry,[87] with many industry leaders refusing to allow their own children to own or use devices,[88] or attend schools where such devices are prevalent.

135. In a recent study, 48% of parents of 5- to 8-year-olds reported difficulty getting their children to turn off mobile devices.[89] 26% of teens and 50% of kids age 8-12 report that their parents monitor what they do on their digital devices through an app or other tools.[90] Parents are increasingly concerned about their children's mobile device usage, and for good reason: research has associated increasing usage with negative consequences for children,[91] such as increasing rates of ADHD,[92] depression,[93] anxiety,[94] and reduced focus in the classroom.[95] One recent study showed that children between the ages of 12 and 18 who spent more time playing games had lower than average social-emotional well-being.[96]

---

[87] *See, e.g.*, Farhad Majoo, "It's Time for Apple to Build a Less Addictive iPhone," New York Times (Jan. 17, 2018), https://www.nytimes.com/2018/01/17/technology/apple-addiction-iphone.html (last accessed July 30, 2021) ("Tech 'addiction' is a topic of rising national concern."); Thuy Ong, "Sean Parker on Facebook: 'God only knows what it's doing to our children's brains'," The Verge (Nov. 9, 2017), https://www.theverge.com/2017/11/9/16627724/sean-parker-facebook-childrens-brains-feedback-loop (last accessed July 30, 2021) (former tech industry leader recognizing that app creators intentionally "exploit[] human vulnerabilities" to increase app engagement).

[88] Nick Bilton, "Steve Jobs Was a Low-Tech Parent," New York Times (September 10, 2014), https://www.nytimes.com/2014/09/11/fashion/steve-jobs-apple-was-a-low-tech-parent.html (last accessed on July 30, 2021); Claudia Dreifus, "Why We Can't Look Away From Our Screens," New York Times (March 6, 2017), https://www.nytimes.com/2017/03/06/science/technology-addiction-irresistible-by-adam-alter.html (last accessed on July 30, 2021).

[89] Media Use By Kids Age Zero To Eight, *supra* at n.65, at 40.

[90] Media Use by Tweens and Teens, *supra* at n.69, at 55.

[91] Ryan M. Atwood et al., Adolescent Problematic Digital Behaviors Associated with Mobile Devices, 19 North American J. Psychology 659-60 (2017) (collecting studies); *Id.* at 672-73 (finding that more than 82.5% of teens were classified as over-users of the Internet, and finding that mobile device usage increased Internet usage).

[92] Nicholas Kardaras, Glow Kids 123-124 (2016).

[93] *Id.* at 127.

[94] *Id.*; 60 Minutes, "Brain Hacking",https://www.youtube.com/watch?v=awAMTQZmvPE (last accessed on July 30, 2021).

[95] Glow Kids, *supra* at n.80, at 123.

[96] Media Use by Tweens and Teens, *supra* at n.69, at 79.

136. Most parents believe that children are better off spending less time on their mobile devices.[97] Three out of four parents are worried about their children's use of screen devices.[98] A recent study showed that 67% of parents of children under age 8 worry about companies collecting data about their children through media, while 69% are concerned about too much advertising.[99]

137. Such fear is well-founded. The World Health Organization ("WHO") recently added "gaming disorder" to its globally-recognized compendium of medical conditions and diagnoses. In the 11th International Classification of Diseases, the WHO describes the condition as "impaired control over gaming, increasing priority given to gaming over other activities to the extent that gaming takes precedence over other interests and daily activities, and continuation or escalation of gaming despite the occurrence of negative consequences."[100]

J. State Privacy Laws Protect Children and Their Parents from Privacy-Invasive Tracking, Profiling, and Targeting of Children Online.

138. Invasion of privacy has been recognized as a common law tort for over a century. *See Matera v. Google Inc*., 15-CV-0402, 2016 WL 5339806, at *10 (N.D. Cal, Sept. 23, 2016) (citing Restatement (Second) of Torts §§ 652A-I for the proposition that "the right to privacy was first accepted by an American court in 1905, and 'a right to privacy is now recognized in the great majority of the American jurisdictions that have considered the question'"). As Justice Brandeis explained in his seminal article, *The Right to Privacy*, "[t]he common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and

[97] Media Use By Kids Age Zero To Eight, *supra* at 134, at 39.
[98] *Id.* at 42.
[99] *Id.*
[100] World Health Organization, "Gaming Disorder", http://www.who.int/features/qa/gaming-disorder/en/ (last accessed Sept. 4, 2018); *see also* Haley Tsukayama, "Video Game Addiction is a Real Condition, WHO Says. Here's What That Means." Washington Post (Jun. 18, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/06/18/video-game-addiction-is-a-real-condition-who-says-heres-what-that-means/?utm_term=.9f718977d0e5 (last accessed July 30, 2021).

emotions shall be communicated to others." Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890). The Second Restatement of Torts recognizes the same privacy rights through its tort of intrusion upon seclusion, explaining that "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy." Restatement (Second) of Torts § 652B (1977). The Supreme Court similarly recognized the primacy of privacy rights, explaining that the Constitution operates in the shadow of a "right to privacy older than the Bill of Rights." *Griswold v. Connecticut*, 381 U.S. 479, 486 (1965).

139. Most recently, the Supreme Court explicitly recognized the reasonable expectation of privacy an individual has in her cell phone, and the Personal Information generated therefrom, in its opinion in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). There, the Court held that continued access of an individual's cell phone location data constituted a search under the Fourth Amendment because "a cell phone—almost a "feature of human anatomy[]"—tracks nearly exactly the movements of its owner . . . A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales . . . Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Id.* at 2218 (internal citations omitted).

140. And, even more recently, the Northern District of California, in an order denying a motion to dismiss an intrusion upon seclusion claim for the exfiltration of children's Personal Information in different mobile apps, held that "current privacy expectations are developing, to say the least, with respect to a key issue raised in these cases – whether the data subject owns and controls his or her personal information, and whether a commercial entity that secretly harvests it commits a highly offensive or egregious act." *McDonald v. Kiloo ApS*, 358 F. Supp. 3d 1022, 1035 (N.D. Cal. 2019). The *McDonald* court's reasoning was subsequently adopted in the District of

New Mexico in analogous litigation. *See New Mexico ex rel. Balderas v. Tiny Lab Prods*., 457 F. Supp. 3d 1103, 1127 (D.N.M. 2020), *on reconsideration*, No. 18-854 MV/JFR, 2021 WL 354003 (D.N.M. Feb. 2, 2021).

141. It is precisely because of our devices' capacity for "near perfect surveillance" that courts have consistently held that time-honored legal principles recognizing a right to privacy in one's affairs naturally apply to online monitoring.

1. The Surreptitious and Deceptive Collection of Personal Information Violates Children's Reasonable Expectations of Privacy and is Highly Offensive.

142. A reasonable person believes the conduct described above violates children's expectations of privacy.

143. A survey conducted by the Center for Digital Democracy ("CDD") and Common Sense Media of more than 2,000 adults found overwhelming support for the basic principles of privacy embedded in state common law, as well as federal law.[101] The parents who were polled responded as follows when asked whether they agreed or disagreed with the following statements:

a. "It is okay for advertisers to track and keep a record of a child's behavior online if they give the child free content."

- 5% strongly agree
- 3% somewhat agree
- 15% somewhat disagree
- **75% strongly disagree**
- 3% do not know or refused to answer

b. "As long as advertisers don't know a child's name and address, it is okay for them to collect and use information about the child's activity online."

- 3% strongly agree
- 17% somewhat agree
- 10% somewhat disagree

[101] Center for Digital Democracy, "Survey on Children and Online Privacy, Summary of Methods and Findings," http://www.centerfordigitaldemocracy.org/sites/default/files/COPPA%20Executive%20Summary%20and%20Findings.pdf (last accessed July 30, 2021).

- **69% strongly disagree**
- 1% do not know or refused to answer

c. "It is okay for advertisers to collect information about a child's location from that child's mobile phone."

- 6% strongly agree
- 3% somewhat agree
- 7% somewhat disagree
- **84% strongly disagree**
- less than 1% do not know or refused to answer

d. "Before advertisers put tracking software on a child's computer, advertisers should receive the parent's permission."

- **89% strongly agree**
- 5% somewhat agree
- 2% somewhat disagree
- 4**%** strongly disagree
- less than 1% do not know or refused to answer

e. When asked, "There is a federal law that says that online sites and companies need to ask parents' permission before they collect personal information from children under age 13. Do you think the law is a good idea or a bad idea?" 93% said it was a good idea, 6% said it was a bad idea, and 1% did not know or refused to answer.

f. Non-parent adults tended to answer in the same way, although parents were more protective of their children's privacy.

144. In a 2013 primer designed for parents and kids to understand their privacy rights online, the CDD noted similar findings:[102]

a. 91% of both parents and adults believe it is not okay for advertisers to collect information about a child's location from that child's mobile phone.

b. 96% of parents and 94% of adults expressed disapproval when asked if it is "okay OK [sic] for a website to ask children for personal information about their friends."

[102] *See* Center for Digital Democracy, "The New Children's Online Privacy Rules: What Parents Need to Know," 6 (June 2013), https://www.democraticmedia.org/sites/default/files/CDDCOPPAParentguideJune2013.pdf (last accessed July 30, 2021).

c. 94% of parents, as well as 91% of adults, believe that advertisers should receive the parent's permission before putting tracking software on a child's computer.

145. In a Pew Research Center study, 79% of adults say they are "at least somewhat concerned about how companies are using the data it collects about them."[103] Specifically, 84% of adults say they are least a little concerned about how much personal information advertisers might know about them.[104]

146. According to the same study, 81% of American "say they have very little or no control over the data collected about them by . . . companies."[105]

147. Smartphone owners are especially active when it comes to these behaviors. Some 50% of smartphone owners have cleared their phone's browsing or search history, while 30% have turned off the location tracking feature on their phone due to concerns over who might access that information.[106] Such behaviors exemplify people's expectation that their personal information—including their location—not be tracked by others online.

148. In another study by the Pew Research Center done as part of its "Internet & American Life" project, respondents were asked, "Which of the following statements comes closest to exactly how you, personally, feel about targeted advertising being used online—even if neither is exactly right?" 68% said, "I'm not okay with it because I don't like having my online behavior tracked and analyzed." 28% said, "I'm okay with it because it means I see ads and get

---

[103] *See* Brooke Auxier, et al., *Americans concerned, feel lack of control over personal data collected by both companies and the government*, Nov. 15, 2019, https://www.pewresearch.org/internet/2019/11/15/americans-concerned-feel-lack-of-control-over-personal-data-collected-by-both-companies-and-the-government/ (last accessed July 30, 2021).

[104] *Id.*

[105] *Id.*

[106] Jan Lauren Boyles, et al., *Privacy and Data Management on Mobile Devices*, Pew Research Center, Sept. 5, 2012, http://www.pewinternet.org/files/old-media//Files/Reports/2012/PIP_MobilePrivacyManagement.pdf (last accessed July 30, 2021).

information about things I'm really interested in."[107] Thus, more often than not, attitudes toward data collection for use in targeted advertising are negative.

149. A survey of 802 parents and their age 12 to17 year-old teenage children showed that "81% of parents of online teens say they are concerned about how much information advertisers can learn about their child's online behavior, with some 46% being 'very' concerned."[108]

150. A study comparing the opinions of young adults between the ages of 18 to 23 with other typical age categories (25-34, 35-44, 45-54, 55-64, and 65+) found that a large percentage is in harmony with older Americans regarding concerns about online privacy, norms, and policy suggestions.[109] For example, 88% of young adults surveyed responded that "there should be a law that requires websites and advertising companies to delete all stored information about an individual"; for individuals in the 45-54 age range, 94% approved of such a law.

151. The same study noted that "[o]ne way to judge a person's concern about privacy laws is to ask about the penalties that companies or individuals should pay for breaching them." A majority of the 18-24 year olds polled selected the highest dollar amount of punishment ("more than $2,500") in response to how a company should be fined if it purchases or uses someone's personal information illegally; across all age groups, 69% of individuals opted for the highest fine. Finally, beyond a fine, around half of the sample (across all age groups) chose the harshest

---

[107] Kristen Purcell, et al., *Search Engine Use*, Pew Research Center 2012 http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_Search_Engine_Use_2012.pdf (last accessed July 30, 2021).

[108] Mary Madden, et al., *Parents, Teens, and Online Privacy*, Pew Research Center 2012, http://www.pewinternet.org/files/old-media//Files/Reports/2012/PIP_ParentsTeensAndPrivacy.pdf (last accessed July 30, 2021).

[109] Chris Hoofnagle, et al., *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies?* (2010), http://ssrn.com/abstract=1589864 (last accessed July 30, 2021).

penalties for companies using a person's information illegally—putting them out of business and jail time.

152. Another study's "findings suggest that if Americans could vote on behavioral targeting today, they would shut it down." The study found that 66% of 1000 polled individuals over the age of 18 did not want online advertisements tailored for them, and that when the same individuals were told that tailored advertising was "based on following them on other websites they have visited," the percentage of respondents rejecting targeted advertising shot up to 84%.[110]

153. Even when consumers are told that online companies will follow them "anonymously," Americans are still averse to this tracking: 68% definitely would not allow it, and 19% would probably not allow it.

154. The study found that 55% of 18-24 year old Americans rejected tailored advertising when they were not informed about the mechanics of targeted advertising. As with the general sample, the percentage of rejections shot up to 67% when those 18-24 year olds were informed that tailored advertising was based on their activities on the website they are visiting, and then 86% when informed that tailored ads were based on tracking on "other websites" they had visited. Despite the overwhelming aversion to targeted advertising, these findings suggest that public concern about privacy-intrusive targeted advertising is *understated* based on the fact that the public may not fully understand how a targeted advertisement is delivered to it. When properly understood by consumers, targeted advertising, and the tracking and profiling in the background, is decried across all age groups.

155. A survey on consumer expectations in the digital world, conducted by Deloitte's Technology, Media & Telecommunications practice[111] and based on polling conducted in 2017 of

---

[110] Joseph Turow, et al., *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It* (2009), http://ssrn.com/abstract=1478214 (last accessed July 30, 2021).

[111] Kevin Westcott, et al., *Digital Media Trends Survey: A New World of Choice for Digital*

2,088 individuals (from the following age groups: ages 14-20 (born 1997-2003); ages 21-34 (born 1983-1996); ages 35-51 (born 1966-1982); ages 52-70 (born 1947-1965); ages 71+ (born 1946 or earlier) found:

a. 73% of all U.S. consumers indicated they were concerned about sharing their personal information online and the potential for identity theft.

b. In 2017, there was a 10-point drop in willingness to share personal data in exchange for personalized advertising (from 37% to 27%).

c. The reason for the sudden change in U.S. consumers' attitudes is they overwhelmingly lack confidence in companies' ability to protect their data: 69% of respondents across generations believe that companies are not doing everything they can to protect consumers' personal data.

d. 73% of all consumers across all generations said they would be more comfortable sharing their data if they had some visibility and control. In addition, 93% of U.S. consumers believe they should be able to delete their online data at their discretion.

156. In the same vein, one news organization recently summarized a *Journal of Consumer Research* article, capturing society's discomfort with and feelings of revulsion toward the practice of targeted advertising and the data exfiltration required: "There's something unnatural about the kind of targeting that's become routine in the ad world, this paper suggests, something taboo, a violation of norms we consider inviolable—it's just harder to tell they're being violated online than off. But the revulsion we feel when we learn how we've been algorithmically targeted,

Consumers, Center for Technology, Media & Telecommunications, 12th ed., https://www2.deloitte.com/content/dam/insights/us/articles/4479_Digital-media-trends/4479_Digital_media%20trends_Exec%20Sum_vFINAL.pdf (last accessed July 30, 2021).

the research suggests, is much the same as what we feel when our trust is betrayed in the analog world."[112]

157. By collecting and sharing children's Personal Information in order to profile and track them across multiple online platforms, and failing first to obtain verifiable parental consent, Rovio has breached children's and parents' expectations of privacy.

158. Various other sources provide manifestations of society's deep revulsion toward companies' collecting or accessing personal information for tracking and profiling purposes:

a. Legislative enactments reflect society's growing concern for digital privacy and security. For example, N.M. Stat. Ann. § 50-4-34 provides that employers may not force an applicant to provide access to her online social media accounts as a condition of employment. N.M. Stat. Ann. § 21-1-46 provides the same protections to applicant students in the post-secondary education context. Similarly, New Mexico's data breach notification law—N.M. Stat. Ann. § 57-12C-1, *et seq*.—imposes a duty of care on businesses who collect and maintain citizens' personal data, recognizing the dangers inherent in unknown and unauthorized parties accessing such data.

b. Scholarly literature about the evolution of privacy norms recognizes society's expectation of determining for oneself when, how, and the extent to which information about one is shared with others.

c. Self-regulation agencies in the online advertising industry note the American consumer's reasonable concern with online privacy (92% of Americans worry about their online data privacy) and the top causes of that concern include Defendant's conduct at issue here: companies collecting and sharing personal information with other companies.[113]

---

[112] Sam Biddle, "You Can't Handle the Truth about Facebook Ads, New Harvard Study Shows" The Intercept (May 9, 2018), https://theintercept.com/2018/05/09/facebook-ads-tracking-algorithm/?utm_source=digg&utm_medium=email) (last accessed July 30, 2021).

[113] TrustArc Blog, Data Privacy is a Major Concern for Consumers (Jan. 28, 2015),

2. Rovio's Breach of Privacy Norms Is Compounded by the Fact That the Angry Birds Gaming Apps Are Targeting, Tracking, and Profiling Children.

159. Rovio's unlawful intrusion into children's privacy is made even more egregious and offensive by the fact that Rovio and its SDKs have targeted and collected *children*'s information, without obtaining verifiable parental consent.

160. Parents' interest in the care, custody, and control of their children is perhaps the oldest of the fundamental liberty interests recognized by society. The history of Western civilization reflects a strong tradition of parental concern for the nurture and upbringing of children in light of children's vulnerable predispositions. Our society recognizes that parents should maintain control over who interacts with their children and how in order to ensure the safe and fair treatment of their children.

161. Because children are more susceptible to deception and exploitation than adults, society has recognized the importance of providing added legal protections for children, often in the form of parental consent requirements.

162. By way of example, American society has expressed heightened concern for the exploitation of children in numerous ways:

a. At common law, children under the age of eighteen do not have full capacity to enter into binding contracts with others. The law shields minors from their lack of judgment, cognitive development, and experience.

b. At the federal level, and as discussed above, COPPA protects, *inter alia*, children's Personal Information from being collected and used for targeted advertising purposes without parental consent, and reflects a clear nationwide norm about parents' expectations to be involved in how companies profile and track their children online.

---

https://www.trustarc.com/blog/2015/01/28/data-privacy-concern-consumers/ (last accessed July 30, 2021).

c. Under the federal Family Educational Rights and Privacy Act of 1974 ("FERPA"), students have a right of privacy regarding their school records, but the law grants parents a right to access and disclose such records. 20 U.S.C. § 1232g(a)(4).

d. Under state law, New Mexico has expressly adopted and codified the privacy and consent protections for student data also afforded by FERPA in its own state analog: N.M. Code R. § 6.29.1.9.

163. Legislative commentary about the need for federal law to provide protections for children provides another expression of society's expectation that companies should not track *children* online without obtaining parental consent. For example, when discussing the need for federal legislation to protect children's privacy—which eventually led to Congress passing COPPA—Senator Richard Bryan (the primary author of the COPPA bill) stated: "Parents do not always have the knowledge, the ability, or the opportunity to monitor their children's online activities, and that is why Web site operators should get parental consent prior to soliciting personal information. The legislation that Senator McCain and I have introduced will give parents the reassurance that when our children are on the Internet they will not be asked to give out personal information to commercial Web site operators without parental consent."[114]

164. More recently, Senators Edward J. Markey and Richard Blumenthal introduced a bill, the KIDS Act, and stated that "Big Tech has designed their platforms to ensnare and exploit children for more likes, more views, and more purchases."[115]

---

[114] *S. 2326: Children's Online Privacy Protection Act of 1998*, Hearing before Senate Subcommittee on Communications, S. Hrg. 105-1069, at 4 (Sept. 23, 1998) (Statement of Sen. Bryan) (emphasis added).

[115] https://www.markey.senate.gov/news/press-releases/senators-markey-and-blumenthal-introduce-first-of-its-kind-legislation-to-protect-children-online-from-harmful-content-design-features .

165. The advertising industry's own privacy standards, and the self-regulatory agencies which serve it, also support enhanced protections for children online, including obtaining parental consent.

166. For example, a survey of professionals in the advertising industry found that a "substantial majority of [advertising professionals] (79%) agrees that the collection of personal information of children should be prohibited," and over "[h]alf of the advertisers (56.8%) agree with this statement if teenagers are concerned."[116]

167. Further, "[t]he majority of advertisers agree with the statement that parents should give their permission for the data collection of their children (89.5%) and teenagers (78.9%)."

168. In the same vein, the Children's Advertising Review Unit, an arm of the advertising industry's self-regulation branch, recommends that companies take the following steps, *inter alia*, to meet consumers' reasonable expectations of privacy and avoid violating the law:[117]

a. Advertisers have special responsibilities when advertising to children or collecting data from children online. They should take into account the limited knowledge, experience, sophistication, and maturity of the audience to which the message is directed. They should recognize that younger children have a limited capacity to evaluate the credibility of information, may not understand the persuasive intent of advertising, and may not even understand that they are being subjected to advertising.

b. Operators should disclose passive means of collecting information from children (*e.g.*, navigational tracking tools, browser files, persistent identifiers, etc.) and what information is being collected.

---

[116] Kristien Daems, Patrick De Pelsmacker & Ingrid Moons, Advertisers' perceptions regarding the ethical appropriateness of new advertising formats aimed at minors, J. Marketing Comms. 8 (2017).

[117] Children's Advertising Review Unit, *Self-Regulatory Program for Children's Advertising* (2014), http://www.asrcreviews.org/wp-content/uploads/2012/04/Self-Regulatory-Program-for-Childrens-Advertising-Revised-2014-.pdf (last accessed on July 30, 2021).

c. Operators must obtain "verifiable parental consent" before they collect, use, or disclose personal information to third-parties, except those who provide support for the internal operation of the website or online service and who do not use or disclose such information for any other purpose.

d. To respect the privacy of parents, operators should not maintain in retrievable form information collected and used for the sole purpose of obtaining verifiable parental consent or providing notice to parents, if consent is not obtained after a reasonable time.

e. Operators should ask screening questions in a neutral manner so as to discourage inaccurate answers from children trying to avoid parental permission requirements.

f. Age-screening mechanisms should be used in conjunction with technology, *e.g.*, a session cookie, to help prevent underage children from going back and changing their age to circumvent age-screening.

169. By failing to: (1) obtain verifiable parental consent; (2) disclose to parents the nature of their data collection practices; and (3) take other steps to preclude children from accessing apps that surreptitiously capture their personal information, Rovio has breached parents' and their children's reasonable expectations of privacy, in contravention not only of COPPA, but also of privacy norms that are reflected in consumer surveys, centuries of common law, state and federal statutes, legislative commentaries, industry standards and guidelines, and scholarly literature.

V. CLAIMS FOR RELIEF

COUNT I

Children's Online Privacy Protection Act
15 U.S.C. §§ 6501, *et seq.*

170. The State repeats and realleges all preceding paragraphs contained herein.

171. The Attorney General of the State of New Mexico is authorized to bring a civil action in the name of the State against Rovio to enforce regulations prescribed by COPPA and to secure remedies for violations of such regulations. *See* 15 U.S.C. § 6504.

172. Rovio collected Personal Information from New Mexico children under the age of 13 through the Angry Birds Gaming Apps, which Rovio operates and which are directed to children.

173. In numerous instances, in connection with the acts and practices described above, Rovio collected, used, and/or disclosed Personal Information from children (as defined under 16 C.F.R. § 312.2) in violation of COPPA, including, but not limited to, by:

a. Failing to provide sufficient notice of the information Rovio collects, or is collected on its behalf, online from children, how Rovio and its SDKs use such information, their disclosure practices, and all other required content, in violation of Section 312.4(d) of COPPA, 16 C.F.R. § 312.4(d);

b. Failing to provide *any* direct notice to parents of the information Rovio collects, or information that has been collected on its behalf, online from children, how Rovio and its SDKs use such information, their disclosure practices, and all other required content, in violation of Section 312.4(b) and (c) of COPPA, 16 C.F.R. § 312.4(b)-(c);

c. Failing to obtain *any* verifiable parental consent before repeatedly collecting or using Personal Information from children for over a decade, in violation of Section 312.5 of COPPA, 16 C.F.R. § 312.5; and

d. Failing to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of Personal Information collected from children, in violation of Section 312.8 of COPPA, 16 C.F.R. § 312.8.

174. Each collection, use, or disclosure of a New Mexico child's Personal Information in which Rovio violated COPPA in one or more ways described above constitutes a separate

violation for which the State seeks: (a) an injunction enjoining the practice and requiring compliance with COPPA; (b) damages, restitution and other compensation on behalf of residents of the State; (c) disgorgement; (d) punitive damages; (e) costs of enforcement, including attorneys' fees, expert costs, and other litigation expenses; and (f) such other relief as the Court may consider to be appropriate.

175. Prior to filing this action, the State provided to the FTC written notice of this action and a copy of this Complaint, consistent with the requirements of 15 U.S.C. § 6504.

COUNT II

Violations of the New Mexico Unfair Practices Act
N.M. Stat. Ann. §§ 57-12-1, *et seq*.

176. The State repeats and reallege all preceding paragraphs contained herein.

177. Pursuant to Section 1303(c) of COPPA, 15 U.S.C. § 6502(c), a violation of COPPA constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of the FTC Act.

178. Section 57-12-4 of the New Mexico Unfair Practices Act (UPA) provides that "[i]t is the intent of the legislature that in construing Section 3 [N.M. Stat. Ann. § 57-12-3] of the Unfair Practices Act the courts to the extent possible will be guided by the interpretations given by the federal trade commission and the federal courts."

179. As such, by violating COPPA, Rovio engaged in unfair or deceptive acts or practices in violation of N.M. Stat. Ann. § 57-12-1 *et seq.*

180. Additionally, in violation of N.M. Stat. Ann. § 57-12-1 *et seq.*, Rovio committed unconscionable trade practices by taking advantage of the lack of knowledge, ability, experience of capacity of New Mexico children and their parents, to a grossly unfair degree and to the detriment of New Mexico children and their parents. In passing COPPA, the U.S. Congress recognized that tracking children online takes advantage of the extreme information asymmetry

between operators like Rovio and New Mexico children and their parents. This is why, in part, COPPA contains rigorous notice and verifiable consent requirements that cover the Personal Information at issue in this litigation. 16 C.F.R. § 312.4 (notice); 16 C.F.R. § 312.5 (verifiable parental consent). Rovio willfully and knowingly took advantage of New Mexico children and their parents when it ignored COPPA's requirements and surreptitiously used hidden, non-intuitive technology concealed in the Angry Birds Gaming Apps to exfiltrate children's Personal Information, tracking them across time and the internet for the purpose of psychological and commercial exploitation.

181. Additionally, as detailed above, in violation of N.M. Stat. Ann. § 57-12-1 *et seq.*, Rovio knowingly made and continues to make false and misleading representations and omissions, both directly and indirectly, that may, tend to or do deceive or mislead children who play the Angry Birds Gaming Apps and the parents of those children, including, but not limited to:

a. Failing to state material facts in its marketing (targeted squarely at children) about the exfiltration of Personal Information from all users, including all child users;

b. Failing to state the material fact in its marketing (targeted squarely at children) that according to Rovio's self-serving privacy policy, the Apps are not for young children despite clear public representations to the contrary;

c. Representing that the Apps are of a particular standard, quality, or grade when they are not (*e.g.* knowingly and publicly proclaiming that the Apps are COPPA-compliant when they are not);

d. Representing in its user agreement that a user's transaction with Rovio involves rights or obligations that it does not involve (*e.g.* that the burden of protecting Personal Information of users under the age of 13 falls upon those child users themselves, rather than upon Rovio); and

e. Engaging in deceptive and unconscionable sales practices that take advantage of parents' and children's lack of knowledge regarding the implications of Rovio's privacy policy (*e.g.* that despite Rovio's deliberate targeting of children and public declarations of COPPA compliance, all users of the Apps will have their information collected, including children).

182. Each wrongful act or practice committed by or engaged in by Rovio in violation of the statute is an unfair, deceptive, and/or unconscionable act or practice in the conduct of trade or commerce.

183. Each and every wrongful act or practice committed by or engaged in by Rovio in violation of N.M. Stat. Ann. § 57-12-1 *et seq.*, was in connection with the sale, lease, rental or loan of good or services and the offering for sale, lease, rental or loan of good or services, including in connection with: (a) Angry Birds Gaming Apps marketed and sold to New Mexico children and their parents for paid download; (b) virtual goods or services marketed and sold to New Mexico children and their parents within the Angry Birds Gaming Apps for enhanced play of those apps; (c) physical goods marketed and sold to New Mexico children to induce, encourage and provide access to the Angry Birds Gaming Apps by New Mexico children; and (d) the sale of targeted advertising services published within the Angry Birds Gaming Apps and powered by the Personal Information exfiltrated from New Mexico children.

184. Rovio's violations were, and are, willful, deceptive, unfair, and unconscionable. Rovio is aware of the violations yet has failed to adequately and affirmatively take steps to cure the misconduct.

185. Rovio's willful violations justify assessing civil penalties of up to $5,000 for each violation of the UPA.

186. The State has determined that Rovio is using, and has used, methods, acts, and practices prohibited by the UPA, such that the imposition of an injunction against Rovio

prohibiting the conduct set forth herein is in the public interest. Therefore, to prevent Rovio from continuing to engage in the violations as set forth herein, the State hereby seeks temporary and permanent injunctions prohibiting Rovio from engaging in the unfair, deceptive, and unconscionable policies, practices, and conduct described in this Complaint.

187. Rovio further is liable to the State for restitution, in an amount to be determined at trial, arising out of Rovio's deceptive and/or unfair methods, acts, and practices.

COUNT III

Intrusion Upon Seclusion

188. The State repeats and realleges all preceding paragraphs contained herein.

189. New Mexico brings this claim in its *parens patriae* capacity pursuant to New Mexico's quasi-sovereign interest in the health and well-being of its residents. New Mexico possesses an interest in this matter apart from the interests of private parties. New Mexico acts herein as a representative of its citizens to redress injuries that affect the general population of New Mexico in a substantial way.

190. Citizens of New Mexico have reasonable expectations of privacy in their mobile devices and their online behavior, generally. New Mexico citizens' private affairs include their behavior on their mobile devices as well as any other behavior that may be monitored by the surreptitious tracking employed or otherwise enabled by the Angry Birds Gaming Apps.

191. The reasonableness of such expectations of privacy is supported by Rovio's unique position to monitor New Mexico citizens' behavior through its access to these individuals' private mobile devices. It is further supported by the surreptitious, highly-technical, and non-intuitive nature of Rovio's tracking.

192. Rovio intentionally intruded on and into New Mexico citizens' solitude, seclusion, or private affairs by intentionally designing the Angry Birds Gaming Apps and the embedded

SDKs to surreptitiously obtain, improperly gain knowledge of, review, and/or retain New Mexico citizens' activities through the monitoring technologies and activities described herein.

193. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia*, the legislation enacted by Congress including COPPA itself, rules promulgated and enforcement actions undertaken by the FTC, and countless studies, op-eds, and articles decrying the online tracking of children. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing New Mexico citizens' personal information with potentially countless third-parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly offensive nature of Rovio's conduct is the fact that Rovio's principal goal was to surreptitiously monitor New Mexico citizens—in one of the most private spaces available to an individual in modern life—and to allow third-parties to do the same.

194. New Mexico citizens were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

195. Rovio's actions and conduct complained of herein were a substantial factor in causing the harm suffered by New Mexico citizens.

196. As a result of Rovio's actions, the State seeks injunctive relief in the form of Rovio's cessation of tracking practices in violation of COPPA and destruction of all Personal Information obtained in violation of COPPA.

197. As a result of Rovio's actions, the State seeks nominal and punitive damages in an amount to be determined at trial. The State seeks punitive damages because Rovio's actions—which were malicious, reckless, oppressive, and willful and/or wanton—were calculated to injure New Mexico citizens and made in conscious disregard of New Mexico citizens' rights. Punitive damages are warranted to deter Rovio from engaging in future misconduct.

VI. PRAYER FOR RELIEF

WHEREFORE, the State respectfully requests that this Court:

A. Enter a permanent injunction to prevent future violations and remedy ongoing and past violations of COPPA, the FTC Act, the UPA and the common law tort of intrusion upon seclusion;

B. Award the State damages, restitution, disgorgement, punitive damages or other compensation on behalf of residents of the State, and such other relief as the Court may consider to be appropriate, for each violation of COPPA;

C. Award the State monetary civil penalties from Defendant;

D. Award the State punitive damages;

E. Award reasonable attorneys' fees and also expenses attributable to both investigating and conducting the litigation; and

F. Award other and additional relief the Court may determine to be just and proper.

Dated: August 25, 2021

Respectfully submitted,

ATTORNEY GENERAL OF NEW MEXICO
HECTOR H. BALDERAS

Brian E. McMath

P. Cholla Khoury
Brian E. McMath
Consumer & Environmental Protection Division
New Mexico Office of the Attorney General
P.O. Drawer 1508
Santa Fe, NM 87504-1508
Phone: (505) 717-3500
Fax: (505) 318-1050
ckhoury@nmag.gov
bmcmath@nmag.gov

Attorneys for Plaintiff